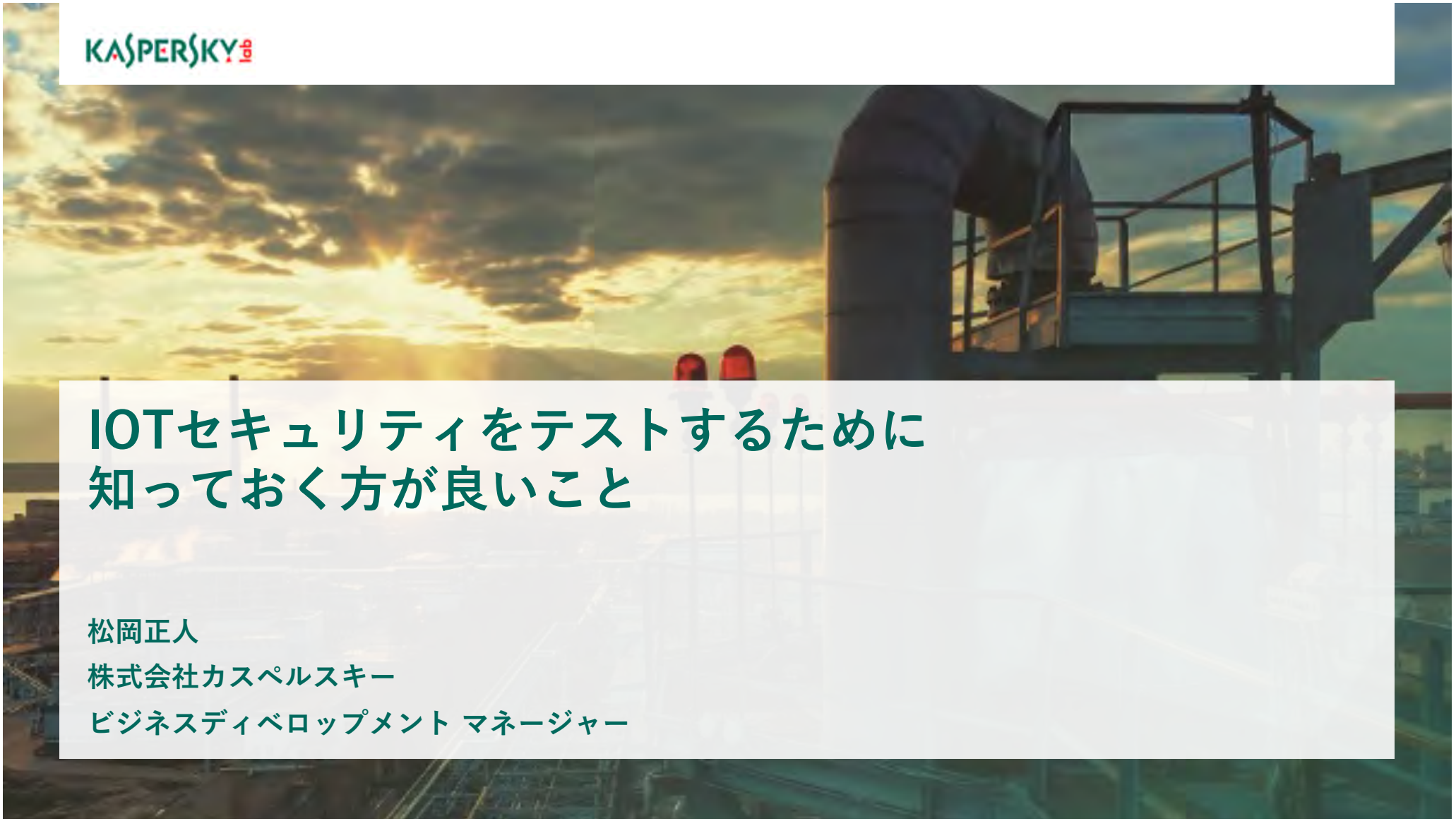


IOTセキュリティをテストするために知っておく方が良いこと

松岡正人
株式会社カスペルスキー
ビジネスディベロップメント マネージャー

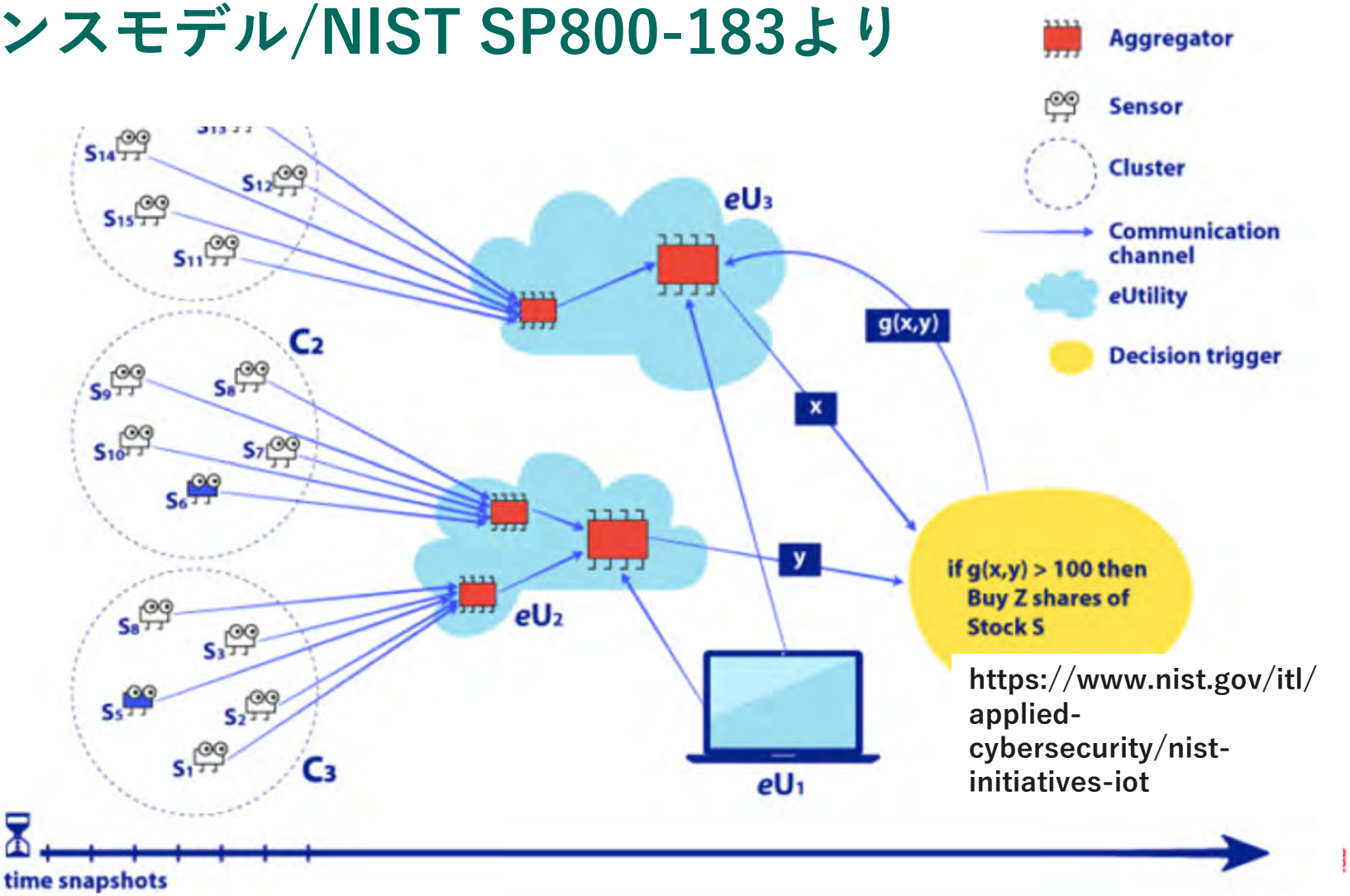
2種類のIOTとセキュリティ

特別ではない
大まかに言うならば
管理できるか
管理できないか

KASPERSKY

アーキテクチャーは NIST SP 800-183を 参照してね

リファレンスモデル/NIST SP800-183より



https://www.nist.gov/itl/applied-cybersecurity/nist-initiatives-iot

セキュリティは NIST SP 800-160を 参照してね

KASPERSKY lab

セキュリティフレームワーク/NIST SP800-160より

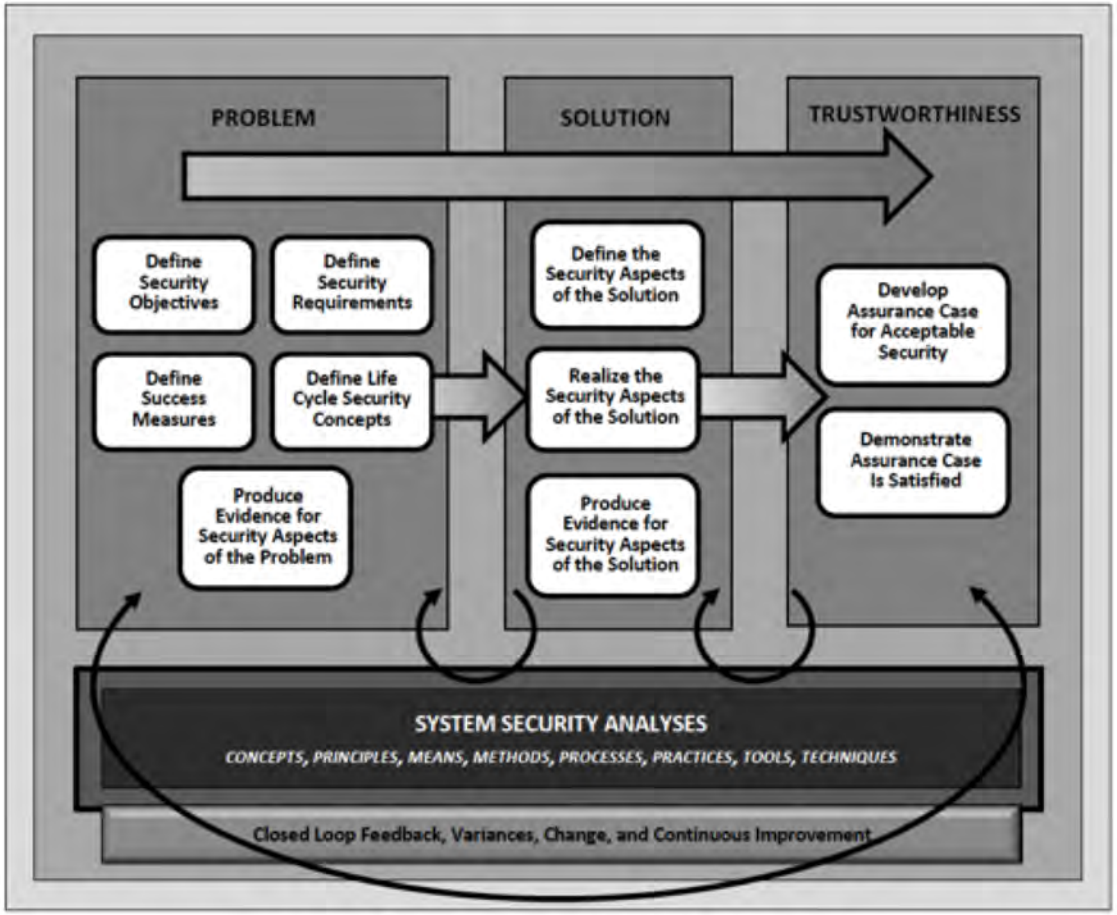


FIGURE 3: SYSTEMS SECURITY ENGINEERING FRAMEWORK

https://www.nist.gov/itl/applied-cybersecurity/nist-initiatives-iot

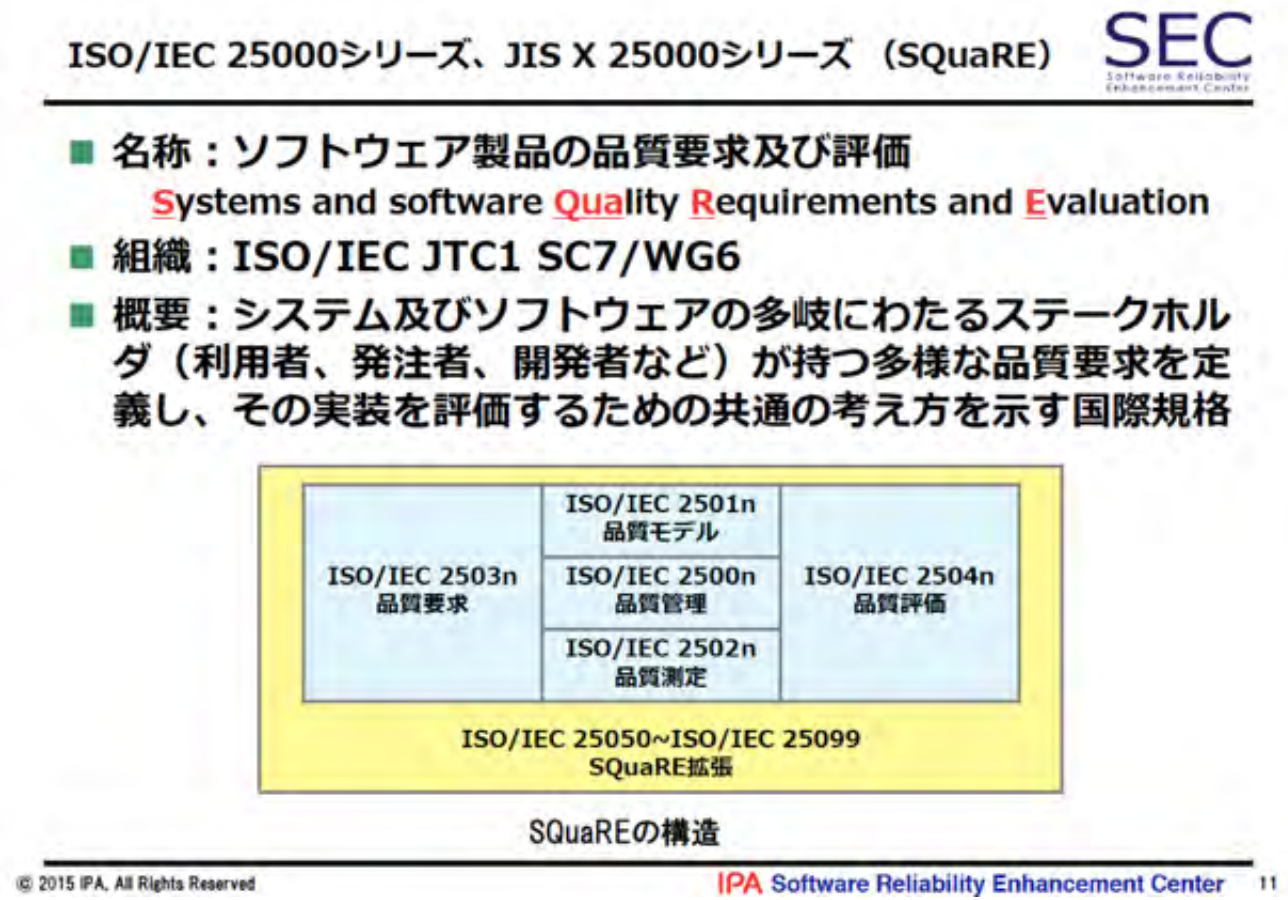
KASPERSKY lab

忘れないで、セキュリティは品質指標のひとつ

JIS X 25000シリーズの品質モデルも参照してね

KASPERSKY

JIS X 25000シリーズ≒ISO/IEC 25000シリーズ



https://www.ipa.go.jp/files/000046839.pdf

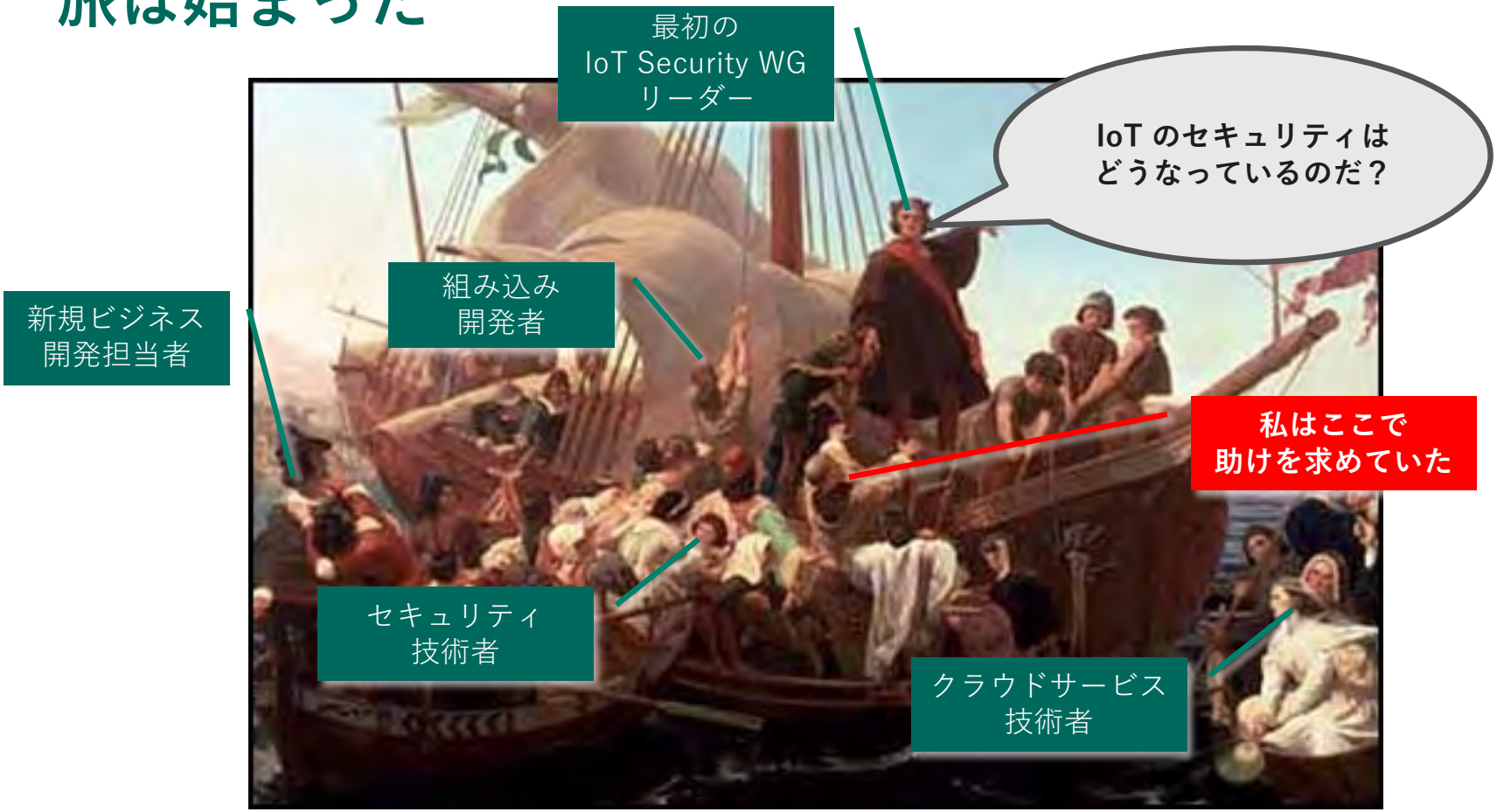
JNSA IOT SECURITY WGの挑戦

管理できないIOT＝コンシューマ向けIOT
コンシューマ向けIoTセキュリティガイドの作成に至る過程

1. Journey has began/旅は始まった
2. What we've found?/何があったのか？
3. Why we've focused on "C"/なぜコンシューマ？
4. Never ending story/終わりのない物語

KASPERSKY

旅は始まった



https://www.pinterest.co.uk/pin/422071796318231297/

KASPERSKY

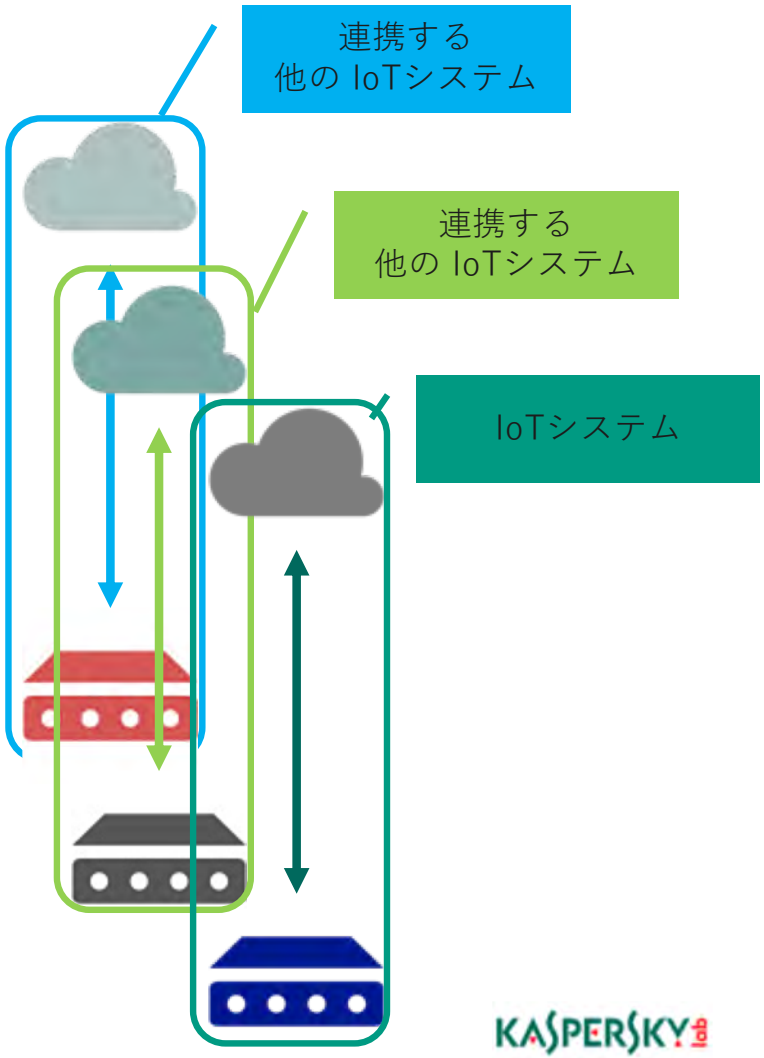
1. Journey has began/旅は始まった
2. **What we've found?/何をみつけたか？**
3. Why we've focused on "C"/なぜコンシューマ？
4. Never ending story/終わりのない物語

KASPERSKY

何をみつけたか？

- 自動車のセキュリティは業界関係者が話しているようだ
  - EVITA、IPA、FMMCなど
- 制御システムもセキュリティの標準化が進められているようだ
  - ISO/IEC、OMG/IIC、TNOなど
- 通信系もいろいろ検討しているようだ
  - oneM2M/ETSI/TTC/ARIB、TIA、CCSAなど
- プロトコルにはセキュリティが徐々にとりこまれてきているようだ
  - MQ TT（いまひとつ）、XMPP（OSSの雄）、AMQP（OASIS）とかとか

で、“IoT” という仕組みを意識して”システム全体” を俯瞰したセキュリティは？



何をみつけたか？

404 error

Good IoT Security Reference is NOT Found except IOT-A

We are sorry but the page you are looking for does not exist.

You could retourn to the homepage or search using the search box below

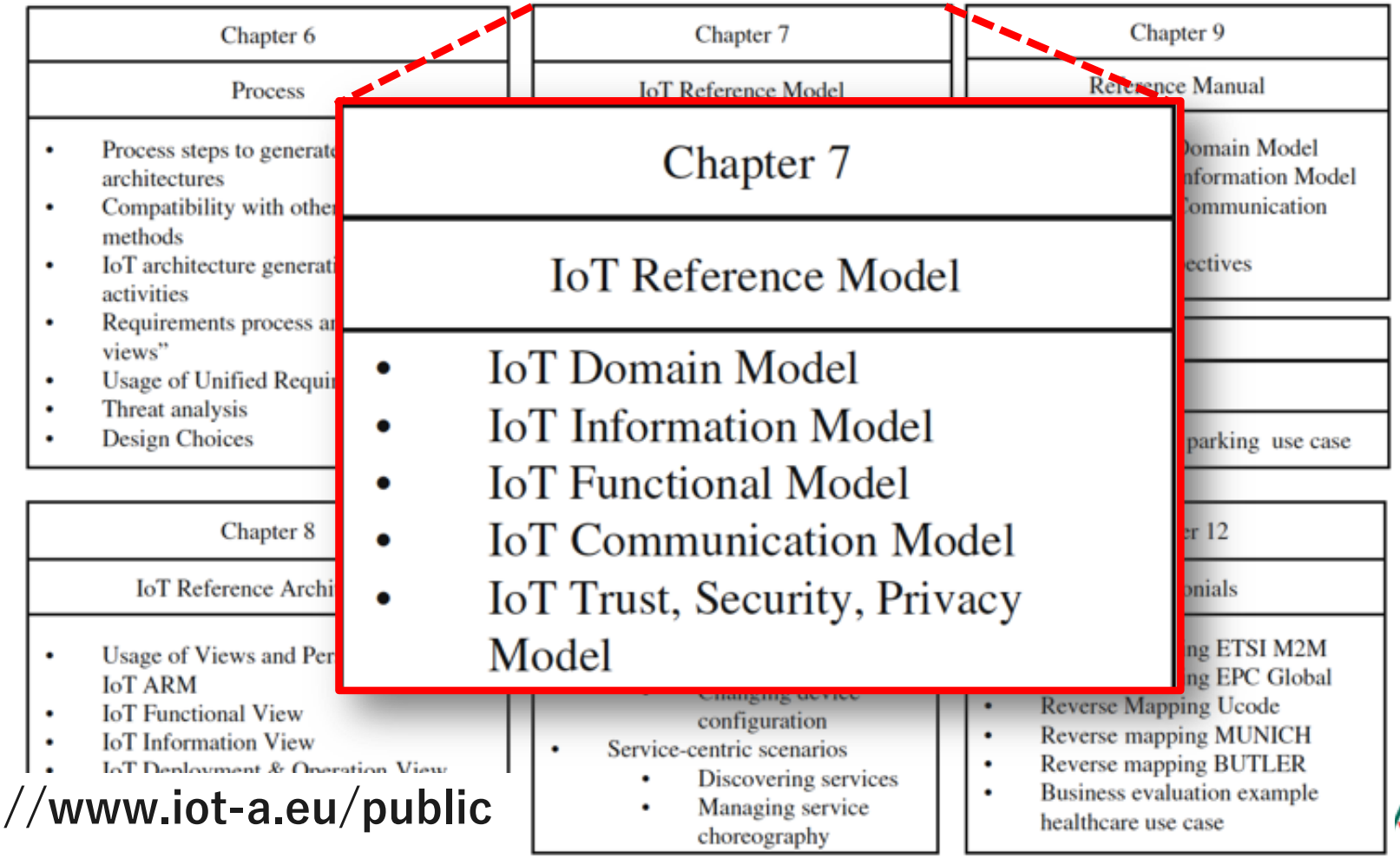
KASPERSKY lab

何をみつけたか？

http://www.iot-a.eu/public

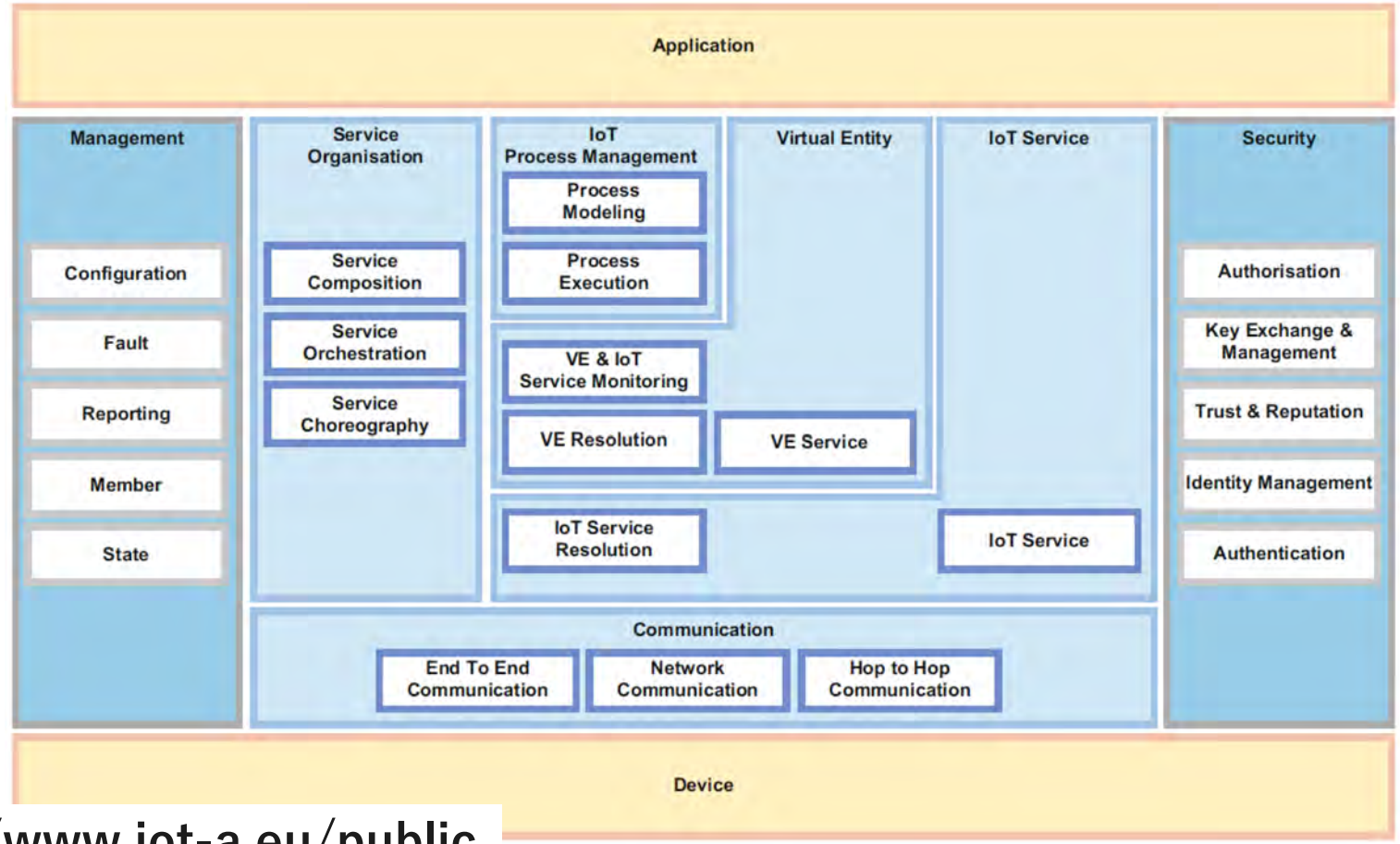
KASPERSKY lab

何をみつけたか？



http://www.iot-a.eu/public

何をみつけたか？



http://www.iot-a.eu/public

KASPERSKY lab

何をみつけたか？

6. Security and privacy

IoT has the potential to change many of our daily activities, routines and behaviours. The physical pervasiveness of the novel sources of information can mean that a great amount of data pertaining to possibly all aspects of human activity – both public and private – will be produced, transmitted, collected, stored and processed. In this scenario it is paramount that users – private citizens, enterprises or public bodies – have the tools to manage their privacy and that their settings are correctly and strongly enforced by security features.

In this context it is useful to define the relationship between security and privacy. A secure system is one that you can trust for sensitive but not necessarily personal information exchange and processing.

Security in information systems is charact

- Authentication (Access restri
- Confidentiality;
- Integrity.

However some security functions used t
to or may be difficult to align with Pr
information. This is the case for principle

- Transparency (Privacy) vs. C
- Verifiability (Privacy) vs. Acc
- Right purpose (Privacy) vs. D

6.1 Privacy

Attention to privacy is rapidly gaining mor
devices and contactless electronic ident
future digital environment. At the same
existence, where everything is connecte

6.2.2.1.2 Physical attacks on RFID

Eavesdropping on the communication

The eavesdropping attack, see Figure 23, is to listen to a private transaction betwee
card without the consent of the protagonists in the intention to uncover secrets. Thi
passive because it does not act on the RFID system. The attack at the physical la
easiest to achieve because it requires very little equipment: a simple field probe an
may be sufficient to recover signals from several meters away. Frames retr
eavesdropping attack will be used to retrieve information. These frames can also be
replay attack. It is of course possible to produce more complex eavesdropping sy
processing in software such as Matlab. Numerous publications deal with this attack,
the test methodology used to obtain their results.

The first results were published in 2004 by the NIST (National Institute of Standards
[367]. NIST researchers were able to retrieve confidential data on a passport locat
spy probe. The equipment used by this team was a commercial reader with a
However, the article gives very little information on test methodology and results
listening distance found by NIST, they have only recovered the data transmitted from
card. Their results also show that the ISO14443 type B would be more susceptible to
ISO14443 type A.

In [367], researchers from BSI (German Federal Office for Information Tech
Information) show that it is possible to listen to communications between an RFID

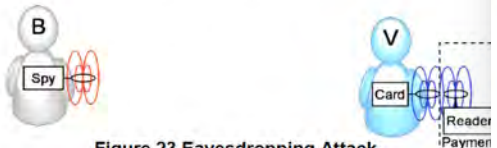


Figure 23 Eavesdropping Attack

from the reader. The reader antenna and antenna system are
tion.

6.2.2.2.3 Neighbor Discovery Attacks

Requirements: A Network Discovery Protocol, malicious node must be part of the network

Self-configuration capabilities in wireless ad-hoc networks are based on Neighborhood Discovery (ND) protocols. The nodes of such networks use these protocols to gather information about the topology of the network and to organize routing. ND protocols use broadcast packets to properly set up the network in the initial deployment and to assess which nodes can be reached directly without the need of a router. **Attacks to the ND protocols** usually rely on making target nodes believe they provide network functionalities (e.g. they are the closest router) in order to alter the proper perception of the network topology and disrupt network traffic, possibly overloading a target node.

The Ipv6 Neighbor Discovery Protocol uses Internet Control Message Protocol Version 6 (ICMPv6) to support Router Discovery, Auto-Configuration of Addresses, Neighbor Un-reachability Detection (NUD protocol), IPv6 Address to Link Layer Resolution, Duplicate Address Detection and Redirection.

NDP features are more rich than IPv4 equivalent set. Moreover, NDP does not feature by default any security features, which makes it vulnerable to a set of attacks.

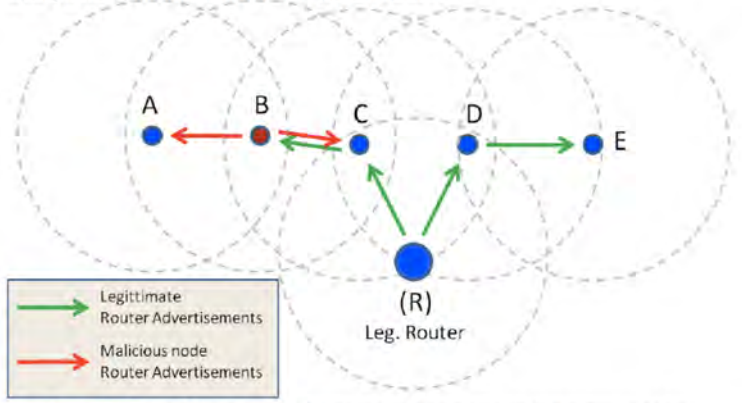


Figure 32: Redirect attack router advertisements from legitimate and malicious nodes

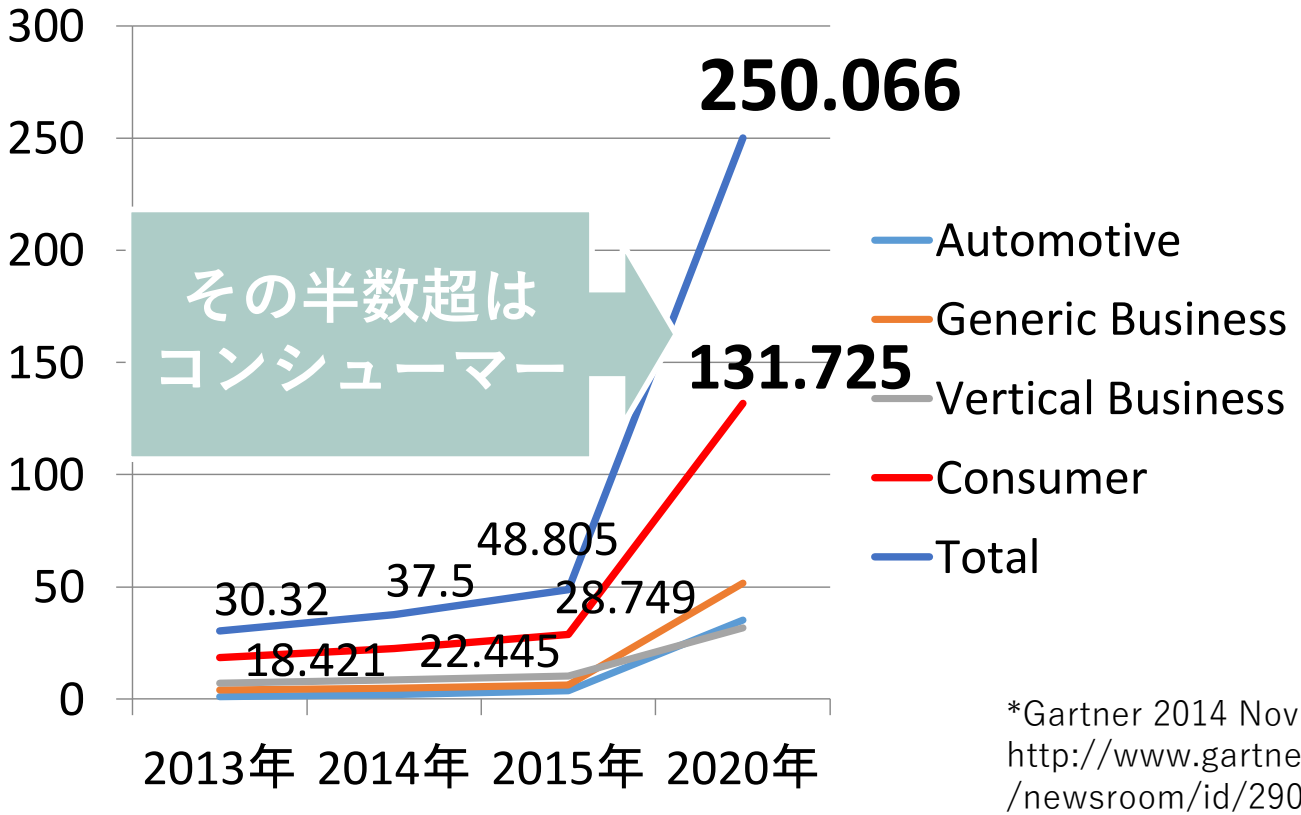
http://www.iot-a.eu/public

KASPERSKY lab

1. Journey has began/旅は始まった
2. What we've found?/何をみつけたか？
3. **Why we'ved focused on "C"/なぜコンシューマ？**
4. Never ending story/終わりのない物語

2020年までに 250億台の IOT

*2014年度予測

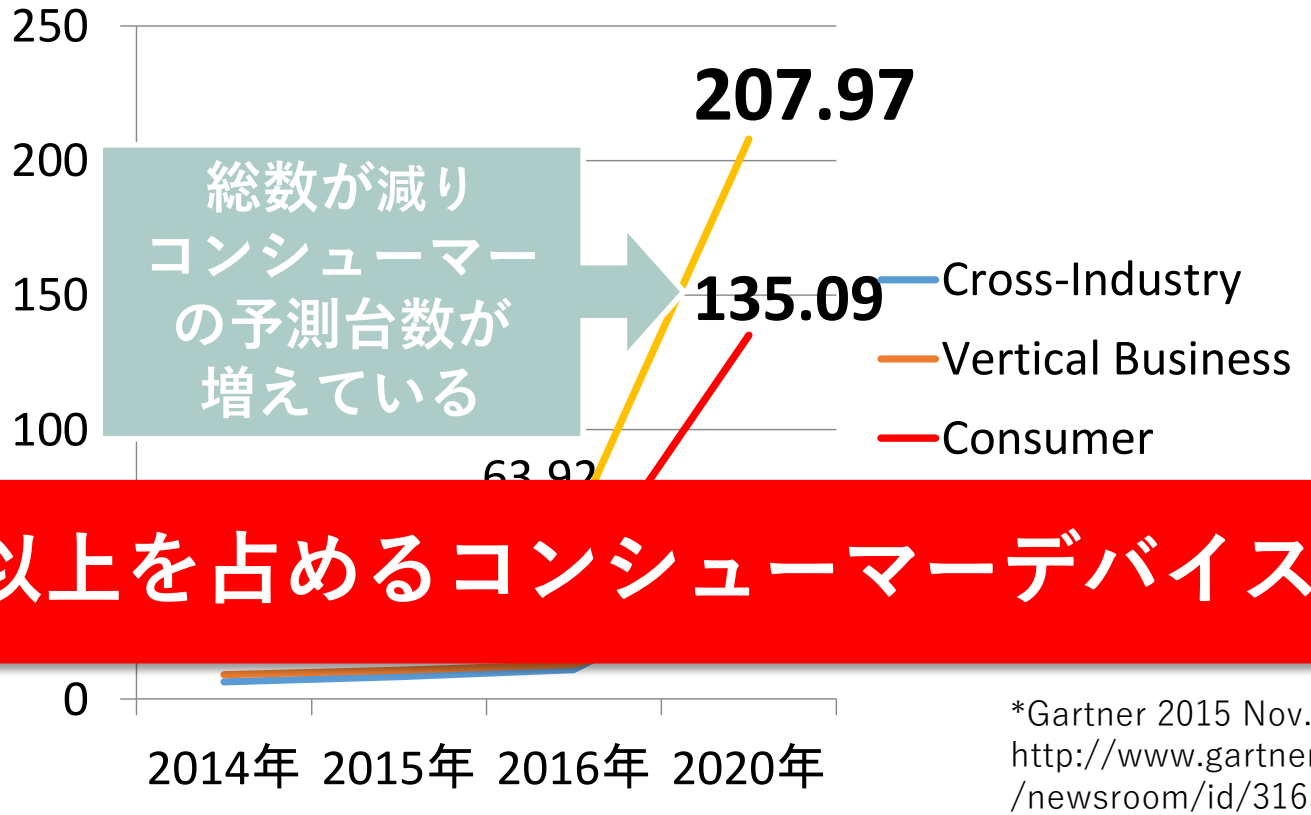


*Gartner 2014 Nov.
http://www.gartner.com
/newsroom/id/2905717

KASPERSKY lab

2020年までに 207億台の IOT

*2015年度予測



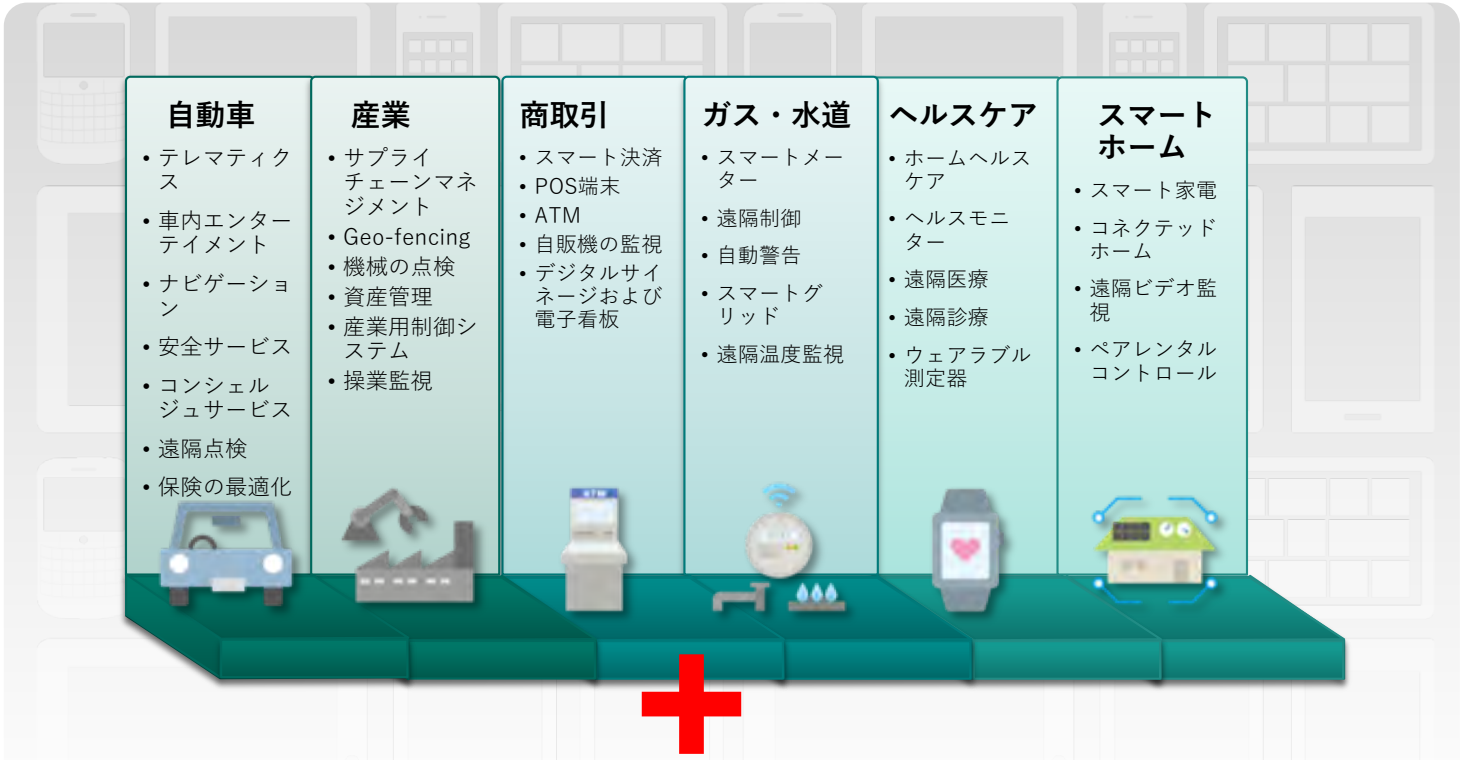
半数以上を占めるコンシューマーデバイスが重要

*Gartner 2015 Nov.
http://www.gartner.com
/newsroom/id/3165317

KASPERSKY

インフラ/産業から個人へ

*INTERNETにつながる機器はより身近に

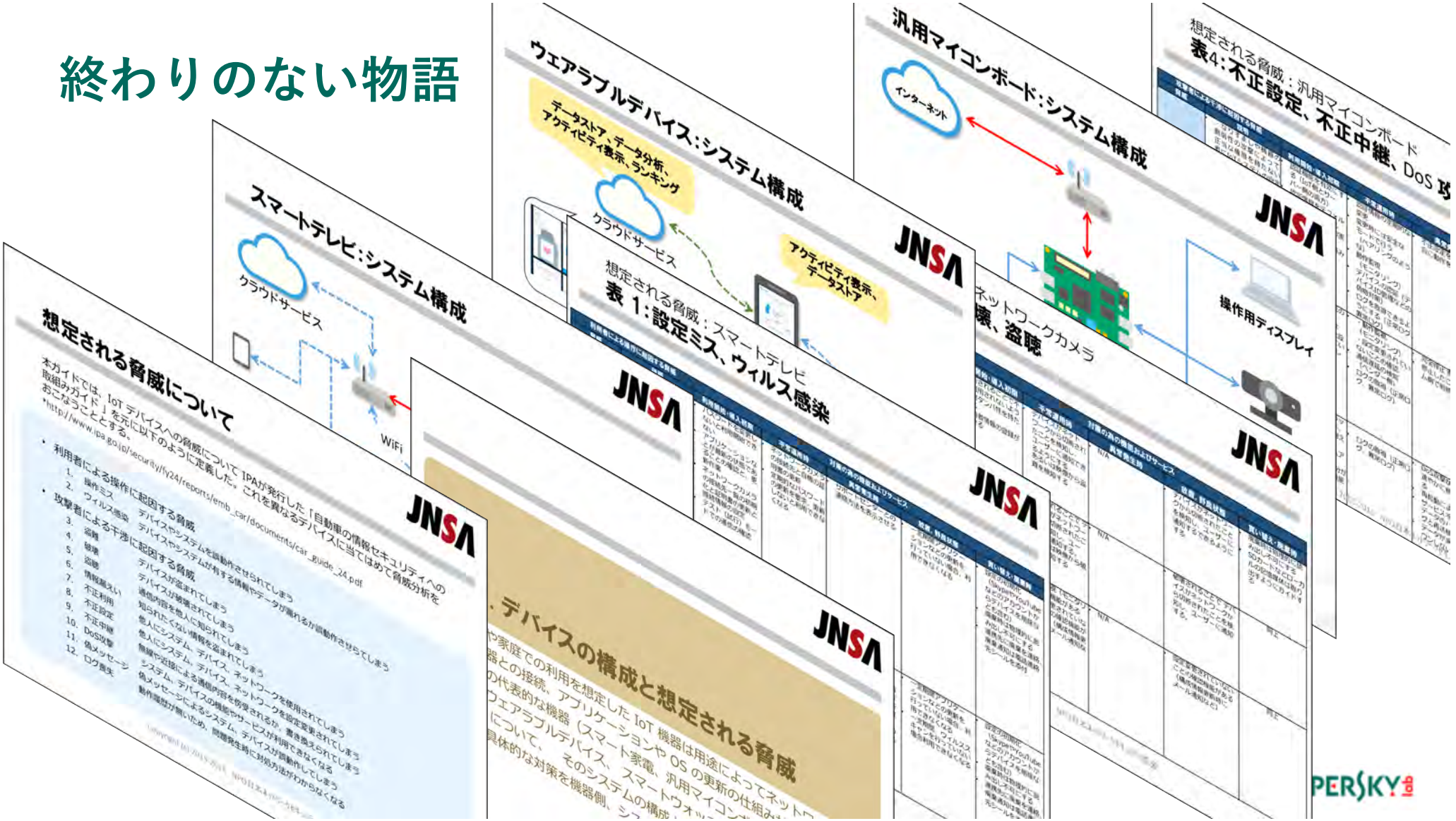


個人用マイコンボード（RaspberryPi など）、ネットワーク玩具 など

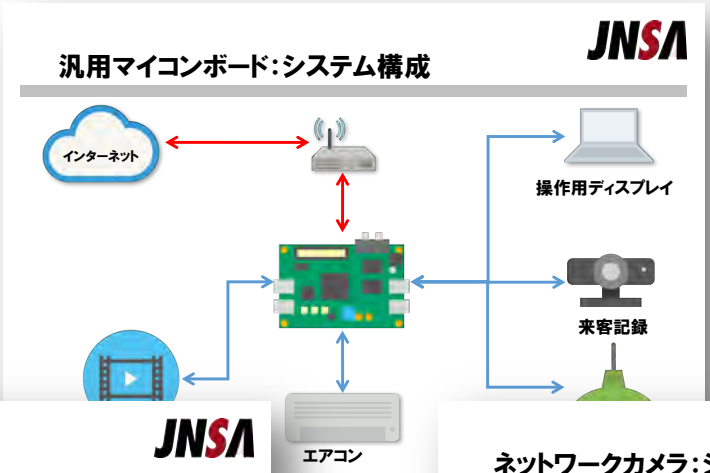
1. Journey has began/旅は始まった
2. What we've found?/何をみつけたか？
3. Why we‘ve focused on “C”/なぜコンシューマ？
4. **Never ending story/終わりのない物語**

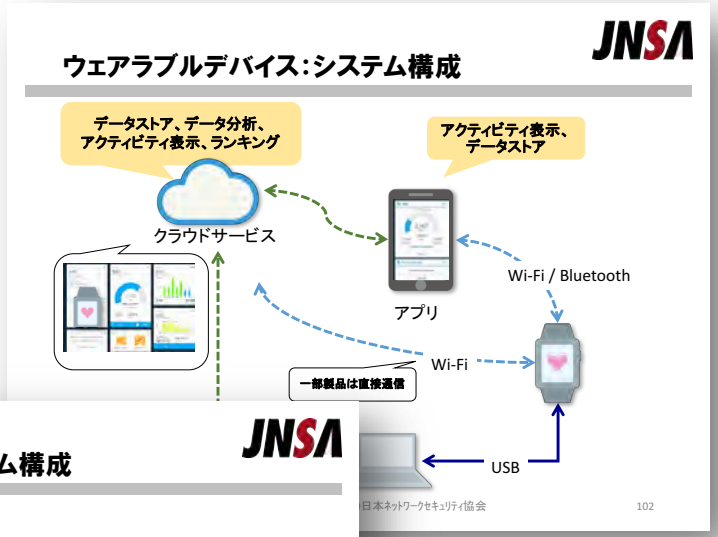
KASPERSKY

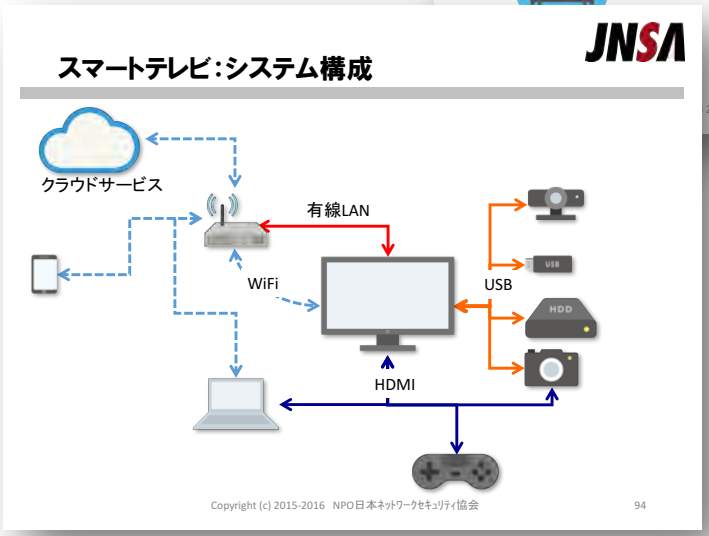
終わりのない物語

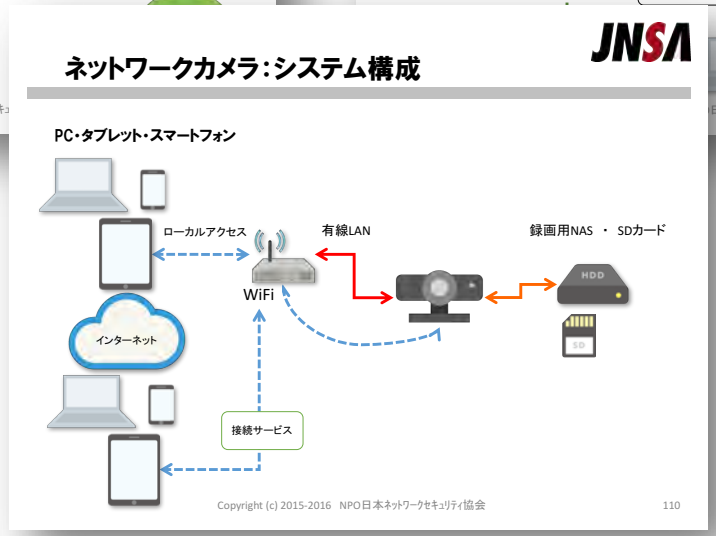

想定される脅威について
スマートテレビ：システム構成
クラウドサービス
WiFi
ウェアラブルデバイス：システム構成
データストア、データ分析、
アクティビティ表示、ランキング
クラウドサービス
アクティビティ表示、
データストア
想定される脅威：スマートテレビ
表 1：設定ミス、ウィルス感染
デバイスの構成と想定される脅威
汎用マイコンボード：システム構成
インターネット
ネットワークカメラ
操作用ディスプレイ
想定される脅威：汎用マイコンボード
表4：不正設定、不正中継、DoS
JNSA
PERSKY lab

終わりのない物語


JNSA
汎用マイコンボード：システム構成
インターネット
操作用ディスプレイ
来客記録
エアコン


JNSA
ウェアラブルデバイス：システム構成
データストア、データ分析、
アクティビティ表示、ランキング
アクティビティ表示、
データストア
クラウドサービス
アプリ
Wi-Fi / Bluetooth
Wi-Fi
一部製品は直接通信
USB
102


JNSA
スマートテレビ：システム構成
クラウドサービス
有線LAN
WiFi
USB
HDMI
HDD
Copyright (c) 2015-2016 NPO日本ネットワークセキュリティ協会
94


JNSA
ネットワークカメラ：システム構成
PC・タブレット・スマートフォン
ローカルアクセス
有線LAN
録画用NAS ・ SDカード
WiFi
インターネット
接続サービス
HDD
SD
Copyright (c) 2015-2016 NPO日本ネットワークセキュリティ協会
110

終わりのない物語

想定される脅威：スマートテレビ
表 1：設定ミス、ウィルス感染

利用者による操作に起因する脅威		対策
脅威	説明	利用開始・導入初期	平常運用時	
操作ミス	・IoTデバイス内のユーザインターフェイスを介して、利用者が行った操作・設定が誤っていたことによりひきおこされる脅威 ・意図しないサービス事業者に個人情報を送付してしまう、通信の暗号機能を OFF にしてしまい通信情報が盗聴される、等	パスワードを変更しないと利用開始できない アプリケーションなどが最新の状態であることの確認と、更新作業 ネットワークカメラの接続先一覧の初期化と証明書の更新と接続情報の設定 テスト（試行）モードでの通信の確認	ネットワークカメラの接続先と自機の証明書の更新 定期的なパスワードの更新を要求、更新しないと利用できなくなる	
ウイルス感染	・利用者が外部から持ち込んだ機器や記録媒体によって、IoTシステムがウイルスや悪意あるソフトウェア（マルウェア等）等に感染することによりひきおこされる脅威 ・IoTデバイスに感染したウイルスがネットワークを通じて更に他のIoTデバイスに感染、等	パスワードを変更しないと利用開始できない 製造元の信頼性の確認 接続可能な外部記憶装置（DLNA）の指定時に可能であればウィルススキャン スマートテレビをつなげようとしているネットワークが感染していないか確認	定期的なウィルスチェック 製造元からの脆弱性情報のチェックとアプリケーションなどが最新の状態であることの確認と、更新作業	不定期のウィルスチェック 製造元からの脆弱性情報のチェックとアプリケーションなどが最新の状態であることの確認と、更新作業 サポートセンターとの連絡方法を表示させる

想定される脅威：スマートテレビ
表 2：盗難、破壊、盗聴

攻撃者による干渉に起因する脅威		対策の為の機能およびサービス			
脅威	説明	利用開始・導入初期	平常運用時	異常発生時	放置、野
盗難	IoTデバイスが盗まれることで、リバースエンジニアリングや、サービスの不正利用などが行われる脅威 IoTデバイスを誰かが持ち去る、など	N/A	スマートテレビがネットワークから切断されたことを検知し、ユーザーに通知し、利用できなくなる	スマートテレビがネットワークから切断されたことを検知し、ユーザーに通知し、利用できなくなる	スマートテレビがネットワークから切断されたことを検知し、ユーザーに通知し、利用できなくなる
破壊	IoTデバイスが破壊されることで、サービスが利用できなくなるか、サービスそのものが提供できなくなる脅威 IoTデバイスが潰されるあるいは燃やされるなどにより使用できなくなる、等	N/A	破壊されることでスマートテレビがネットワークから切断されたことを検知し、ユーザーに通知する	破壊されることでスマートテレビがネットワークから切断されたことを検知し、ユーザーに通知する	破壊されることでスマートテレビがネットワークから切断されたことを検知し、ユーザーに通知する
盗聴	IoTデバイスが有し見られるセンシング情報から得放射途中等				

想定される脅威：スマートテレビ
表3：情報漏洩、不正使用

攻撃者による干渉に起因する脅威		対策の為の機能およびサービス			
脅威	説明	利用開始・導入初期	平常運用時	異常発生時	放置、野
情報漏えい	IoTシステムにおいて保護すべき情報が、許可のされていない者に入手される脅威 蓄積されたコンテンツや各種サービスのユーザ情報が、機器への侵入や通信の傍受によって不正に読み取られる、等	アプリケーションなどが最新の状態であることの確認と、更新作業 ネットワークカメラの接続先一覧の初期化と証明書の更新と接続情報の設定 相互認証方法の確認 Firewallや、侵入検知機能のあるネットワークの利用を推奨し、導入時のオプションとして用意する	記録保存するコンテンツや聴取・録画予約記録などを暗号化する 通信の暗号化 アプリケーションなどが最新の状態であることの確認と、更新作業	異常発生を検知し、ユーザーに通知し、利用できなくなる	記録保存するコンツや聴取・録などを暗号通信の暗号 一定期間アションなど行っていない用できなく 動作監視（モ グ）使用状 視をメーカ スとして提
不正利用	なりすましや機器の脆弱性の攻撃によって、正当な権限を持たない者にIoTシステムの機能などを利用される脅威 認証用の通信をなりすます事により、サービスを不正に利用する、等	アプリケーションなどが最新の状態であることの確認と、更新作業 ネットワークカメラの接続先一覧の初期化と証明書の更新と接続情報の設定 相互認証方法の確認 Firewallや、侵入検知機能のあるネットワークの利用を推奨し、導入時のオプションとして用意する	認証情報の定期的な変更と変更時に専用のモードで行う（ペアリング、二段階認証など） 動作・使用状態の記録と監視をメーカーのサービスとして提供（ウェブサイト経由で確認できるなど） デバイスそのものの偽者などはベンダー側のデバイスID管理などで実現	異常発生を検知し、ユーザーに通知し、利用できなくなる	認証情報の更と変更時モードで行ング、二段など） 動作監視（グ）使用状視をメーカスとして提

想定される脅威：スマートテレビ
表4：不正設定、不正中継、DoS攻撃

JNSA

攻撃者による干渉に起因する脅威		対策の為の機能およびサービス				
脅威	説明	利用開始・導入初期	平常運用時	異常発生時	放置、野良状態	買い替え・廃棄時
不正設定	なりすましや機器の脆弱性の攻撃によって、正当な権限を持たない者にIoTシステムの設定値を不正に変更される脅威 ネットワーク設定を変更し、正常な通信ができないようにする、等	ネットワークカメラの接続先一覧の初期化と証明書の更新と接続情報の設定 相互認証方法の確認 Firewallや、侵入検知機能のあるネットワークの利用を推奨し、導入時のオプションとして用意する	動作・使用状態のログ取得と監視をメーカーのサービスとして提供（ウェブサイト経由で確認できるなど）	異常発生を検知し、ユーザーに通知し、利用できなくなる	動作監視（モニタリング）使用状態の記録と監視をメーカーのサービスとして提供 一定期間アプリケーションなどの更新を行っていない場合、利用できなくなる	物理的に読み出し不可にする 記録保存したコンテンツや各種設定を初期化し、読み出し不可にする
不正中継	通信経路を操作し、正規の通信を乗っ取ったり、不正な通信を混入させる脅威 NFC(RFIDとか)の電波を不正に中継し、攻撃者が車の鍵の通信を鍵の近くから中継して遠隔から鍵を解錠する、等、近接通信であるから安全とした前提を利用するもの	N/A	動作・使用状態の記録と監視をメーカーのサービスとして提供（ウェブサイト経由で確認できるなど）	異常発生を検知し、ユーザーに通知し、利用できなくなる	動作監視（モニタリング）使用状の記録と監視をメーカーのサービスとして提供 一定期間アプリケーションなどの更新を行っていない場合、利用できなくなる	物理的に読み出し不可にする 記録保存したコンテンツや各種設定を初期化し、読み出し不可にする
DoS 攻撃	IoT ゲー 通信 の要 隔制 くさ					

想定される脅威：スマートテレビ
表5：偽メッセージ、ログ喪失（証跡）

JNSA

攻撃者による干渉に起因する脅威		対策の為の機能およびサービス				
脅威	説明	利用開始・導入初期	平常運用時	異常発生時	放置、野良状態	買い替え・廃棄時
偽メッセージ	攻撃者がなりすましのメッセージを送信することにより、IoTシステムに不正な動作や表示を行わせる脅威 エアコンの遠隔操作のメッセージを改ざんし設定温度を高くする、等	相互認証方法の確認 Firewallや、侵入検知機能のあるネットワークの利用を推奨し、導入時のオプションとして用意する	動作・使用状態の記録と監視をメーカーのサービスとして提供（ウェブサイト経由で確認できるなど）	動作・使用状態の記録と監視をメーカーのサービスとして提供（ウェブサイト経由で確認できるなど） 異常発生を検知し、ユーザーに通知し、利用できなくなる	動作・使用状態の記録と監視をメーカーのサービスとして提供（ウェブサイト経由で確認できるなど） 一定期間アプリケーションなどの更新を行っていない場合、利用できなくなる	通信の暗号化 動作・使用状態の記録と監視をメーカーのサービスとして提供（ウェブサイト経由で確認できるなど） 一定期間アプリケーションなどの更新を行っていない場合、利用できなくなる	N/A
ログ喪失（証跡）	操作履歴等を消去または改ざんし、後から確認できなくする脅威 攻撃者が自身の行った攻撃行動についてのログを改ざんし、証拠隠滅を図る、等	動作・使用状態の記録と監視をメーカーのサービスとして提供（ウェブサイト経由で確認できるなど）	動作・使用状態の記録と監視をメーカーのサービスとして提供（ウェブサイト経由で確認できるなど）	動作・使用状態の記録と監視をメーカーのサービスとして提供（ウェブサイト経由で確認できるなど）	動作・使用状態の記録と監視をメーカーのサービスとして提供（ウェブサイト経由で確認できるなど）	物理的に読み出し不可にする 記録保存したコンテンツや各種設定を初期化し、読み出し不可にする

http://www.jnsa.org/result/iot/

KASPERSKY lab

IIC

管理されるIOT=産業用途のIoT=Industrial IoT

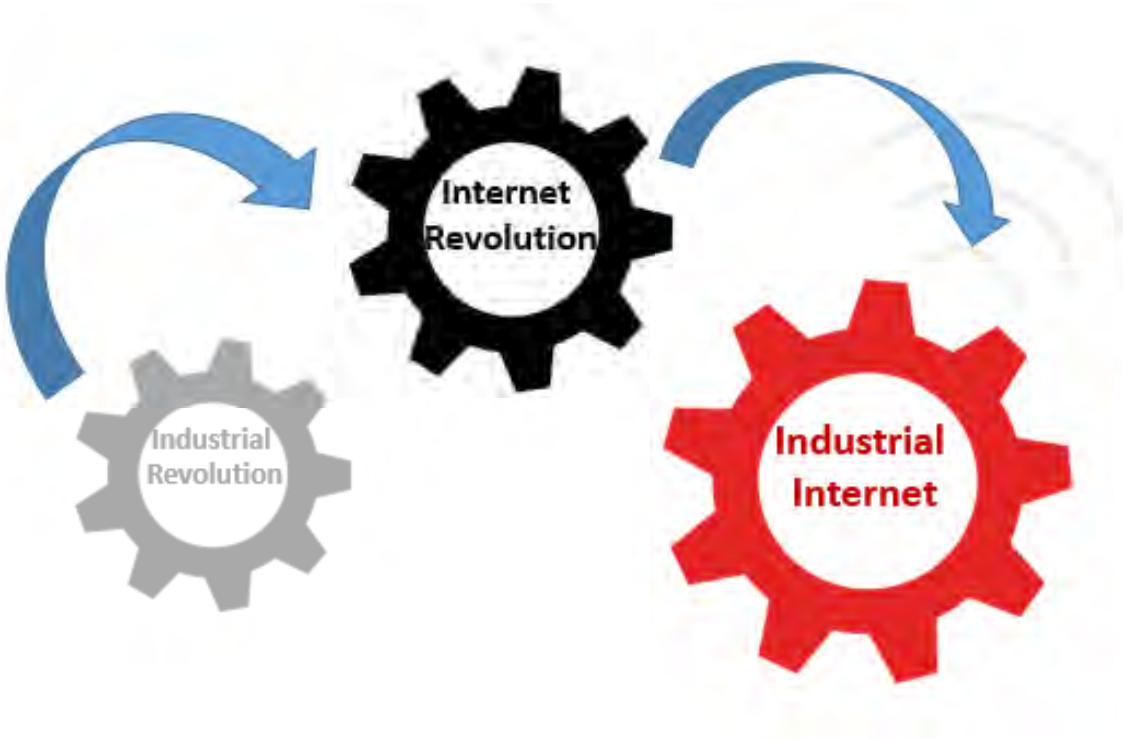
industrial internet CONSORTIUM

IICについて

Industrial Internet Consortium

KASPERSKY lab

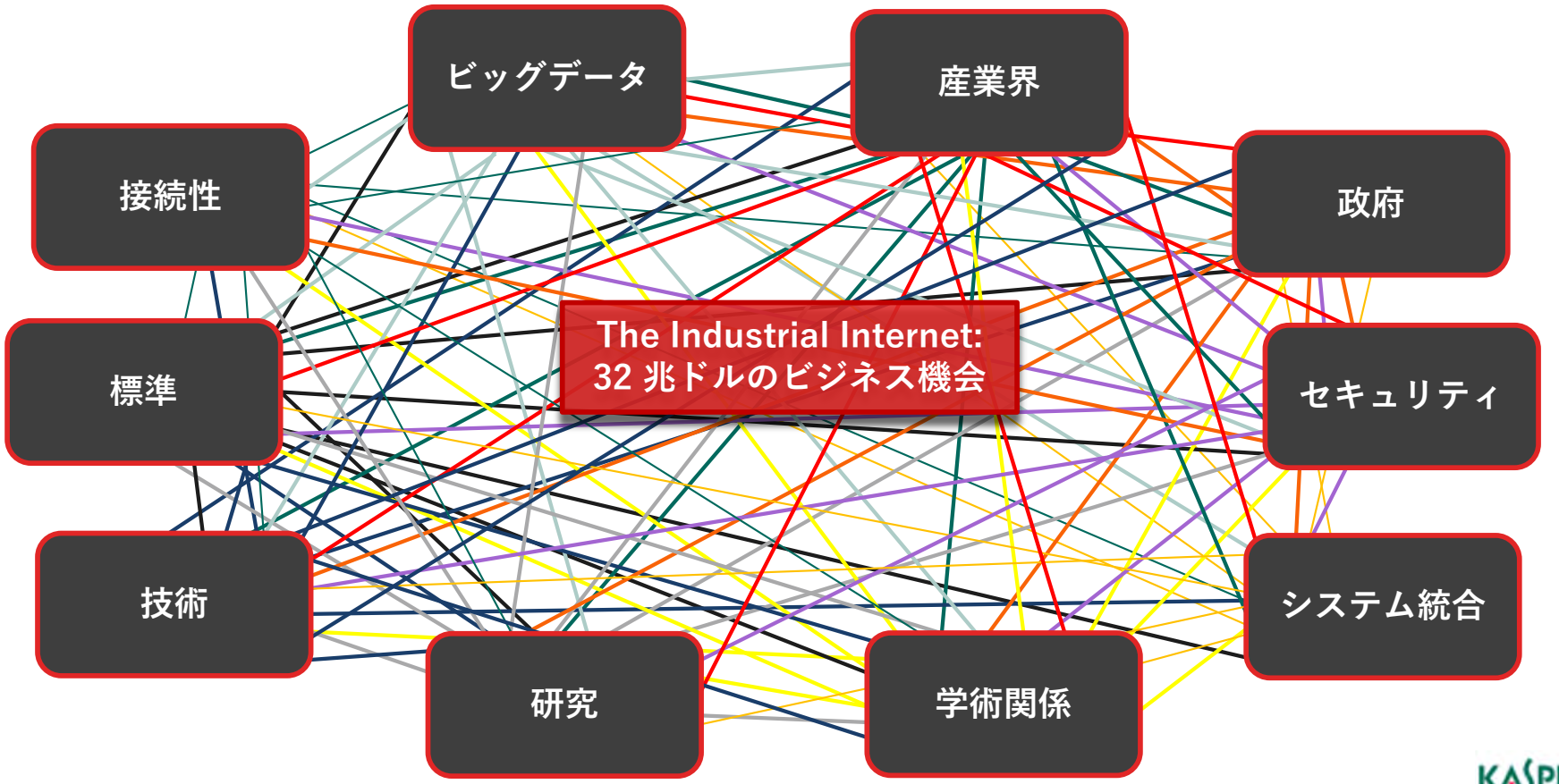
THE INDUSTRIAL INTERNET が新しい経済革命をもたらす



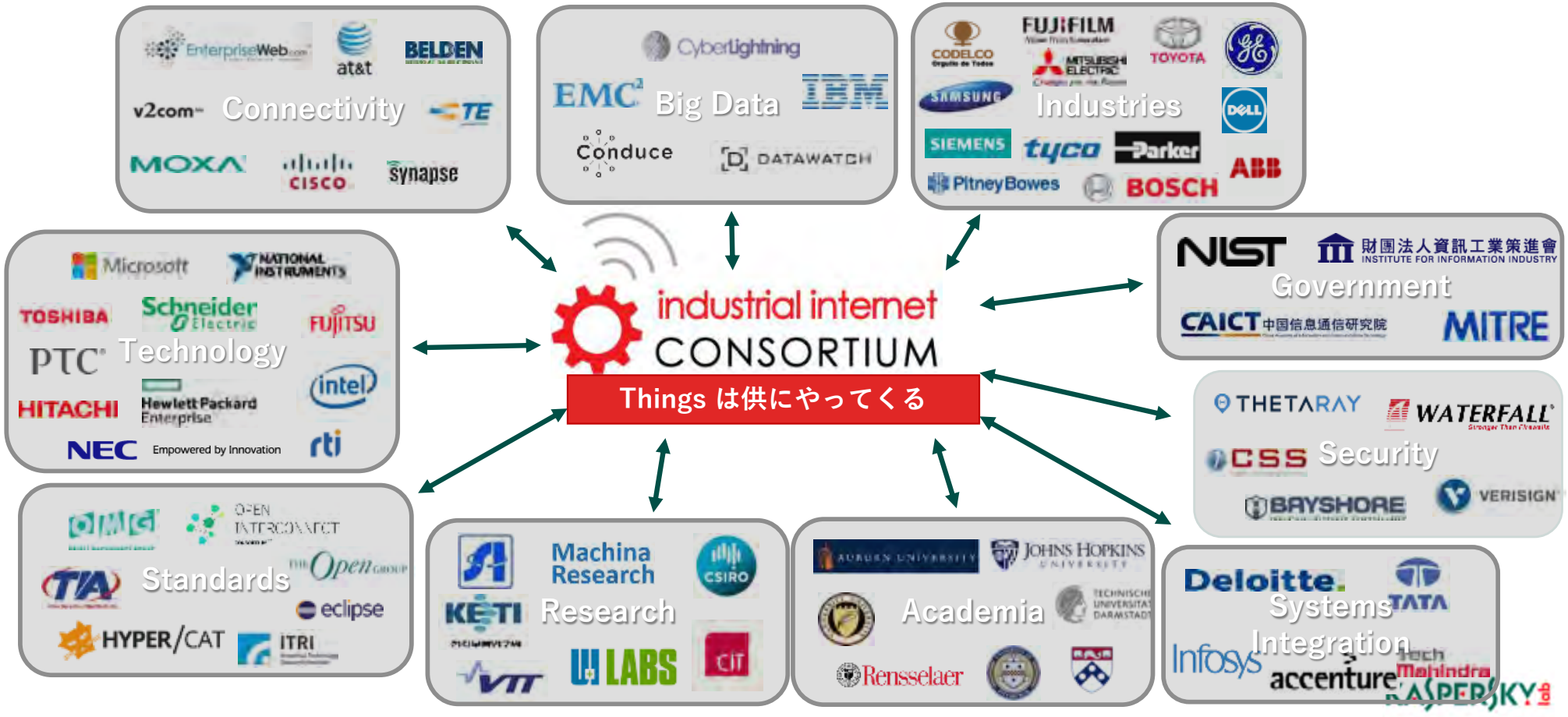
*GDP data extracted from the Futurist 2007

KASPERSKY lab

BRING TOGETHER THE PLAYERS TO ACCELERATE ADOPTION



THE IIC: THINGS ARE COMING TOGETHER



Industrial Internet Consortium の目的

The Industrial Internet Consortium is a global, member
supported organi
growth of the Ind
coordinating eco
control and integ
people, processe
interoperability and open standards to deliver
transformational business and societal outcomes across
industries and public infrastructure.

つまり
新しい経済の仕組みを
一緒に立ち上げましょうということ

250 以上の組織が
30以上の国から参画

- Launched in March 2014 by five founding members:
- AT&T, Cisco, General Electric, IBM & Intel.

- The IIC is an open, neutral “sandbox” where industry, academia and government meet to collaborate, innovate and enable.

INDUSTRIAL INTERNET CONSORTIUM の成果

- テストベッド
  - Track & Trace
  - Time-Sensitive Networking
  - Manufacturing QualityManagement
  - Communication and Control for Microgrid Applications
  - INFINITE
  - The Condition Monitoring andPredictive Maintenance (CM/PM)

など…

- 公開文書
  - Industrial Internet Security Framework
  - Industrial Internet Reference Architecture

など…

*http://www.iiconsortium.org/test-beds.htm

industrial internet CONSORTIUM

IISF

http://www.iiconsortium.org/IISF.htm

KASPERSKY lab

一枚の絵にするならこれ

> KEY SYSTEM CHARACTERISTICS ENABLING TRUSTWORTHINESS

Industryが対象なのでSecurityだけで考えていない

また、Industryだけれど工場などの制御系が主眼ではなく、あらゆる産業が対象なのでPrivacyも含まれるという点で非常に幅広い

e.g. 医療では患者のカルテ情報など

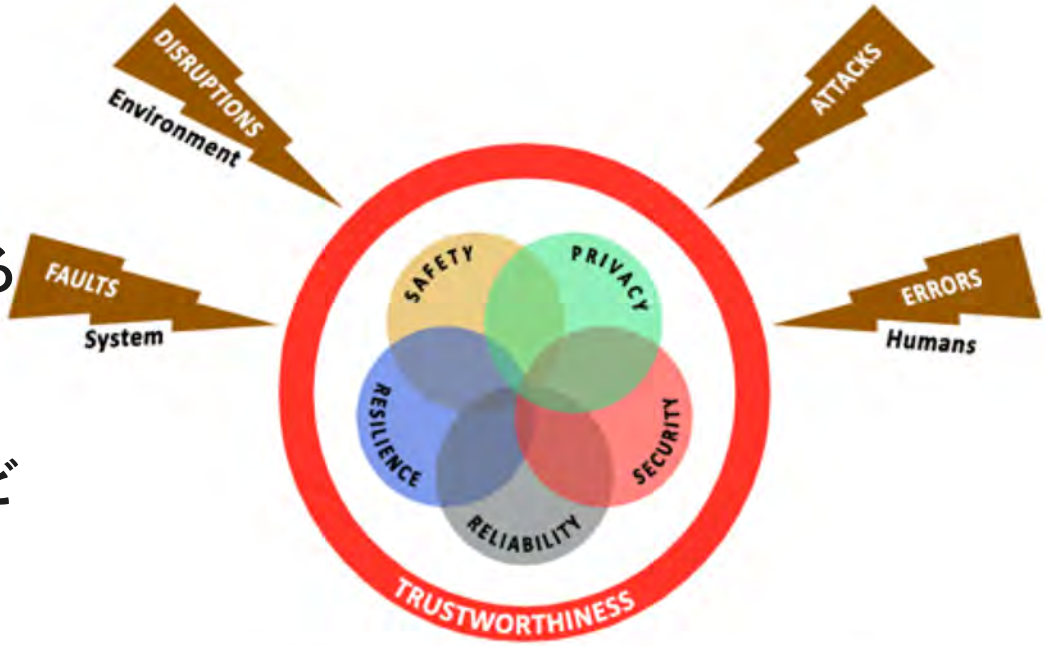


Figure 3-1: Trustworthiness of an IIoT System

TRUSTWORTHINESSとは？

- The degree of confidence one has that the system performs as expected in respect to all the key system characteristics in the face of environmental disruptions, human errors, system faults and attacks. The needs of IT and OT must both be met.

- 信頼度において、環境の環境の破壊、人的エラー、システムの欠陥や攻撃に直面しても、全ての主要なシステムの特徴に関して期待されるシステムの性能を発揮できること。ITとOTのニーズが合致すること。
➔IT/OT双方に求められる信頼性がどのような問題に直面しても発揮されること。

SYSTEM LIFECYCLE

- システムを構成する部品（コンポーネント）の提供者からシステム構築者（ビルダー）だけでなく運用者（ユーザー）も含め、さらに信頼関係も含めたモデルを提示することで役割と責務を明確化

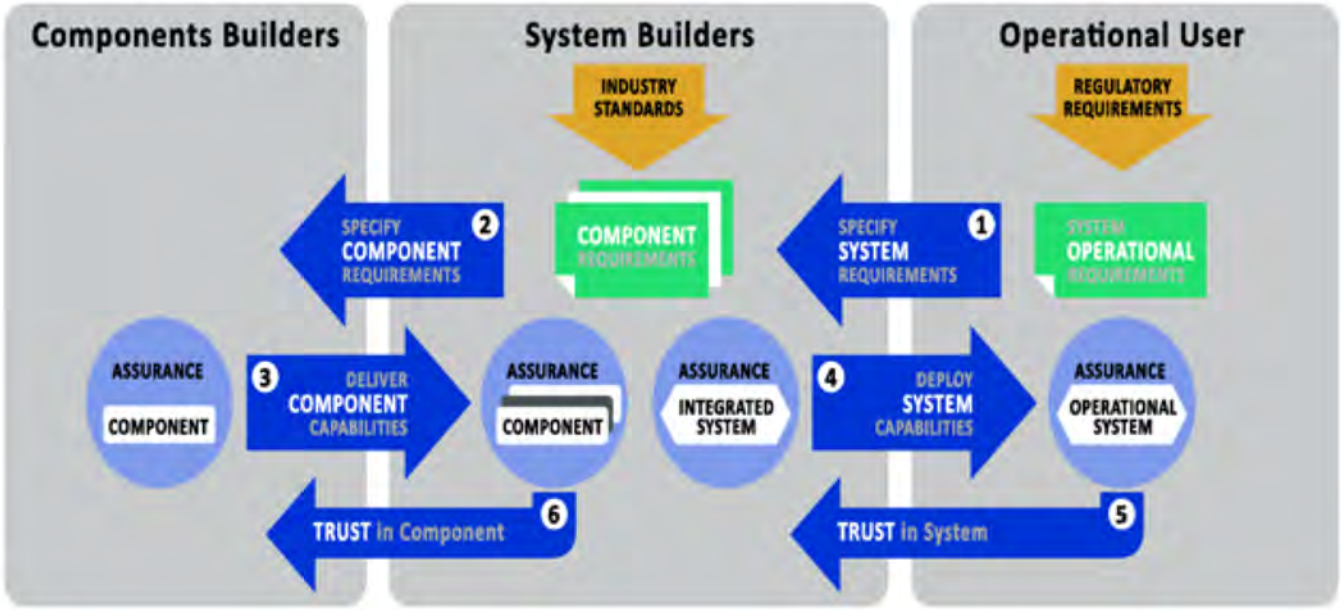


Figure 6-1: Permeation of Trust

The trust lifecycle starts with the specification of requirements that result in the delivery of capabilities. The assurance that these capabilities meet the stated requirements becomes the basis of trust in the system.

TRUST RELATIONSHIP

- 信頼モデルの構築には多数の課題があるとしている

✓要件に例外が列挙しきれない

✓要件はライフサイクルの中で変化する

✓知識や技術の違いで言葉の意味が異なる

✓要件の些細な違いはシステムの大きな差異となる

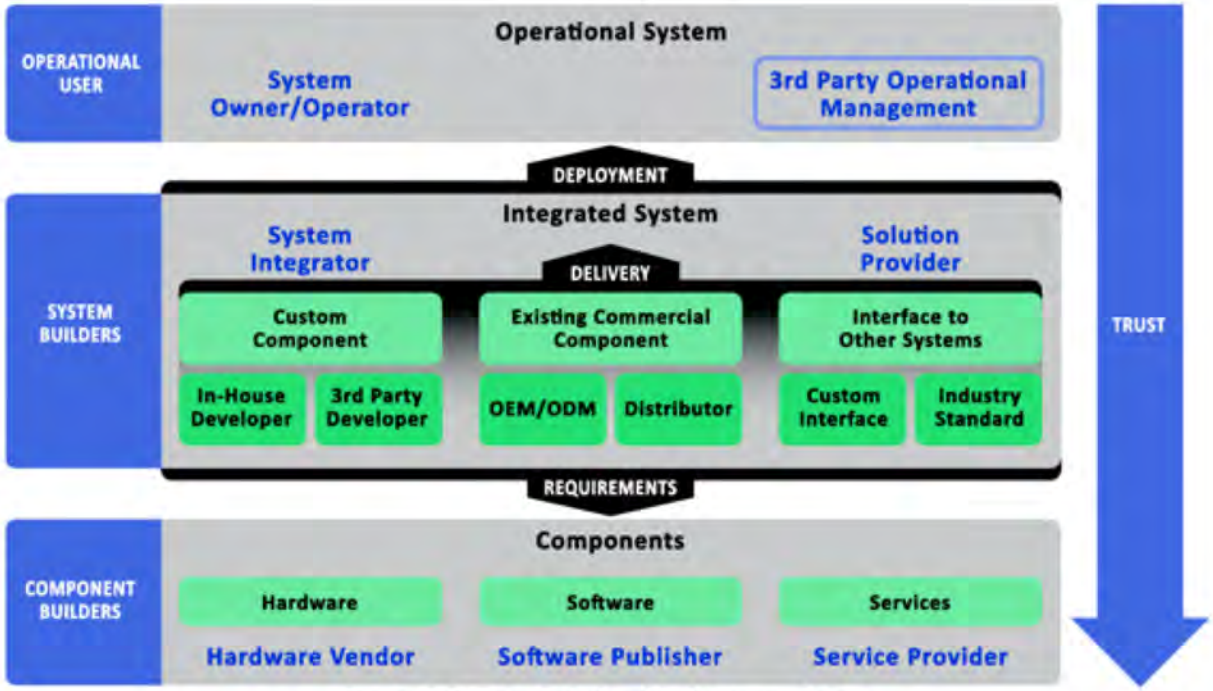


Figure 6-2: Trust Relationship between Actors

KASPERSKY lab

SECURITY THREATS AND VULNERABILITIES ON ENDPOINTS

- エンドポイントを構成するあらゆるものが対象
- OSやAPI、BIOS/UEFIやハードウェアといったシステム構成要素だけでなく、開発環境や管理環境など包括的な視点を提供

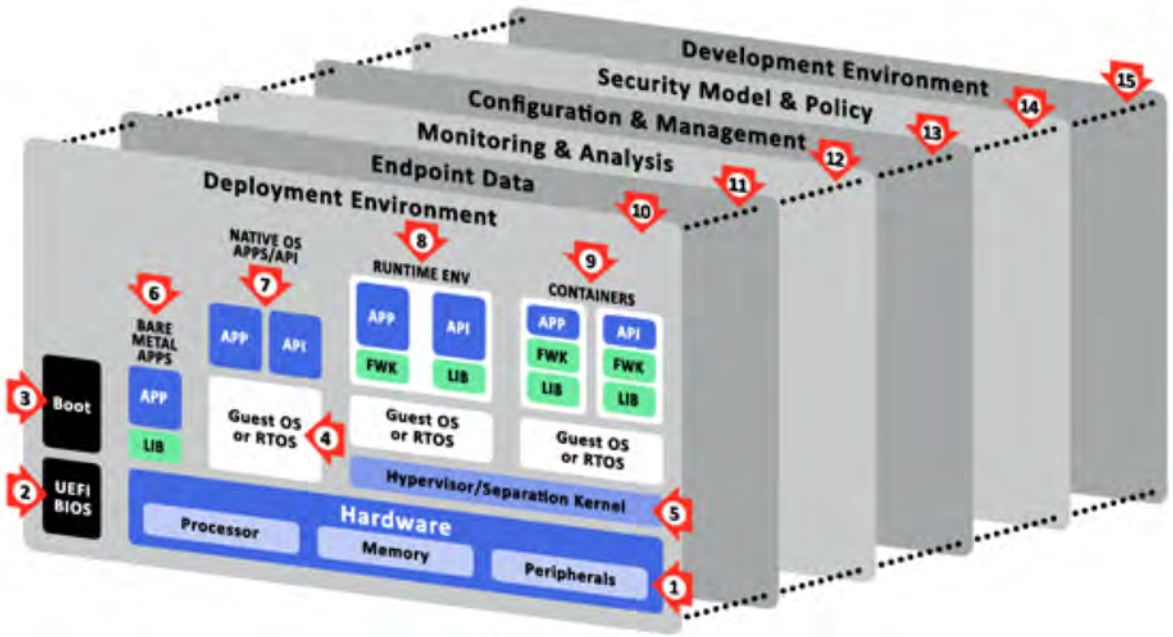


Figure 8-2: Threat and Vulnerabilities to IIoT Endpoints

As shown in Figure 8.2, a broad range of threat and vulnerabilities exist in different facets of the endpoints in each of the following areas:

どうやってセキュリティをテストするのか？

どこから、どうやって、何を？

ペネトレーションテスト（アセスメントの一部でもある）

- セキュリティの世界で「テスト」というとこれ
- でも、いわゆる「ブラックボックステスト」だったりする
- いわゆる「ハッキング」とは違い観察が主体
- しかし「コード解析」や「能動的」に「穴を突く」ことも
- つまり、「ホワイトボックス」＋「グレーボックス」＋「ブラックボックス」というのがこれ
- なんのことはない「脆弱性」を見つけて「リスク評価」することが目的（脆弱性診断とも）

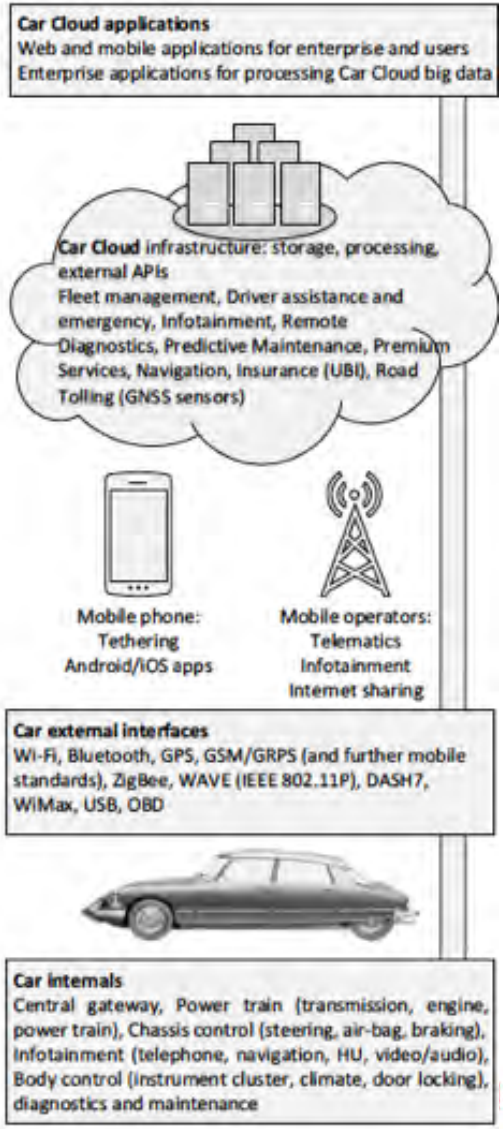
IOTは複合的なシステムとして評価する

- システムアーキテクチャを吟味し脆弱性の境界を見つける
- コンポーネントとシステム全体のテストの評価軸は擦り合わせる
- 更に以下の観点が必要（テストは設計とも置き換え可能）
  - サプライチェーンを考慮したテスト（相互接続されるシステムやユーザー認証などに穴があるか無いか）
  - ライフサイクルを考慮したテスト（OSや基盤アプリの脆弱性が見つかった場合どのような影響があるか、あるいは無いのか）
  - アクセス管理のテスト（ブルートフォースによる管理者権限の乗っ取りなどができるか、などなど）
  - 脆弱性情報の収集と評価（パッチを当ててシステム動くのかとか）

KASPERSKY

例えば車のテスト（アセスメント）

- アプリ・要素毎に評価
  - Car Security Assessment and ECU Security Assessment
  - Application Security Assessment
  - Connected Cars Security Assessment
  - Penetration Testing
  - Telecom Client-side Security Assessment



*Source:Kaspersky AO

CAR SECURITY ASSESSMENT AND ECU SECURITY ASSESSMENT

- 車両セキュリティアセスメント
  - パワートレインサブネットワーク: 変速機、エンジン、伝動機構
  - シャシー制御サブネットワーク: ステアリング、エアバッグ、ブレーキ
  - インフォテイメントサブネットワーク: 電話、ナビ、ヘッドアップビデオ・オーディオ
  - ボディ制御サブネットワーク: 計測器クラスタ、気象検知、ドアロック
  - 診断と保守: 車両全体あるいはコンポーネントのサブセットが分析対象

- ECU セキュリティアセスメント
  - 多様なECU: セントラルGW、Telematics Control Units(TCU)、インフォテイメントシステム、Remote Keyless Entry (RKE) システム、Tire Pressure Monitoring System (TPMS)、盗難防止システム

KASPERSKY

APPLICATION SECURITY ASSESSMENT

- Web アプリケーションセキュリティアセスメント
  - ブラウザー上で動作する関連アプリケーション
- モバイルアプリケーションセキュリティアセスメント
  - iOSやアンドロイドなどの端末で動作するアプリケーション
- 車載アプリケーションセキュリティアセスメント
  - Windows、Linux、VxWorks、QNXなどの各種OS/RTOS 上の各言語で開発されたアプリケーション

KASPERSKY

CONNECTED CARS SECURITY ASSESSMENT

- 対象：
  - 車両追跡
  - 携帯の同期
  - メディア転送
  - 遠隔駐車
  - ファームウェア更新
  - テレメトリーの収集、処理、予測保守など

PENETRATION TESTING

- 外部ペンテスト
  - インターネット経由、事前の知識無しでの評価
- 内部ペンテスト
  - 内部犯行者としてのセキュリティ評価、開発企業のオフィスへの物理的なアクセスを得て、あるいは契約ベンダーとして限定的なアクセス権を得て
- ソーシャルエンジニアリングテスト
  - フィッシング、悪意あるリンク付きのメール、悪意ある添付ファイルなどを利用して情報を窃取するなど
- 無線ネットワークセキュリティアセスメント
  - 現地で（現車）での無線環境の評価試験

KASPERSKY

ペンテスト（アセスメント）のガイドや標準
※たくさんあるけど英語

- Penetration Testing Execution Standard (PTES)：http://www.pentest-standard.org/index.php/Main_Page
- NIST Special Publications 800-115 Technical Guide to Information Security Testing and Assessment：https://csrc.nist.gov/publications/detail/sp/800-115/final
- Open Source Security Testing Methodology Manual (OSSTMM)：http://www.isecom.org/research/
- Information Systems Security Assessment Framework (ISSAF)：http://www.oissg.org/issaf.html
- Web Application Security Consortium (WASC) Threat Classification：http://projects.webappsec.org/w/page/13246978/Threat%20Classification
- Open Web Application Security Project (OWASP) Testing Guide：https://www.owasp.org/index.php/OWASP_Testing_Project
- Microsoft STRIDE Threat Model：https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx

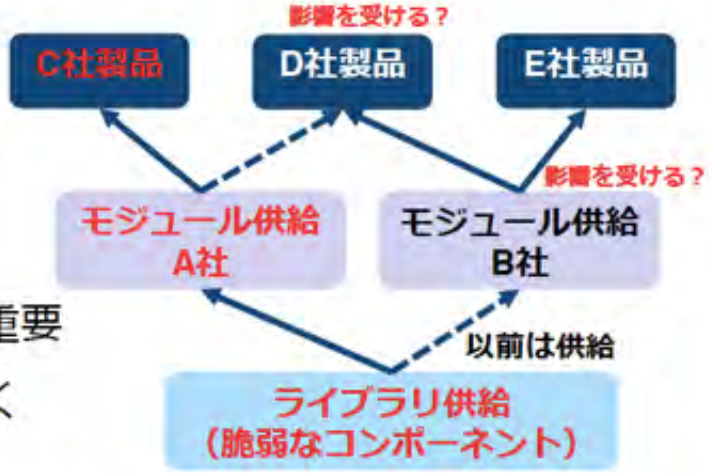
開発中の新しい取り組み

JPCERT/CC、長崎県立大との取り組み「チェックリスト」

脆弱性に対する製品の管理における課題

- **ファームウエアや、サードパーティのライブラリなどでの脆弱性をどう考えるか？**
  - アップデートに対する製造者にかかる責任/負担
  - 最終的な製品がどの脆弱性の影響を受けるのか、影響範囲がどこまでなのかといった脆弱性の管理が必要
  - 開発が大規模になればなるほど、既知の脆弱性対策の反映が困難
    - 脆弱性情報の収集と取り纏め
    - 外部委託先での管理

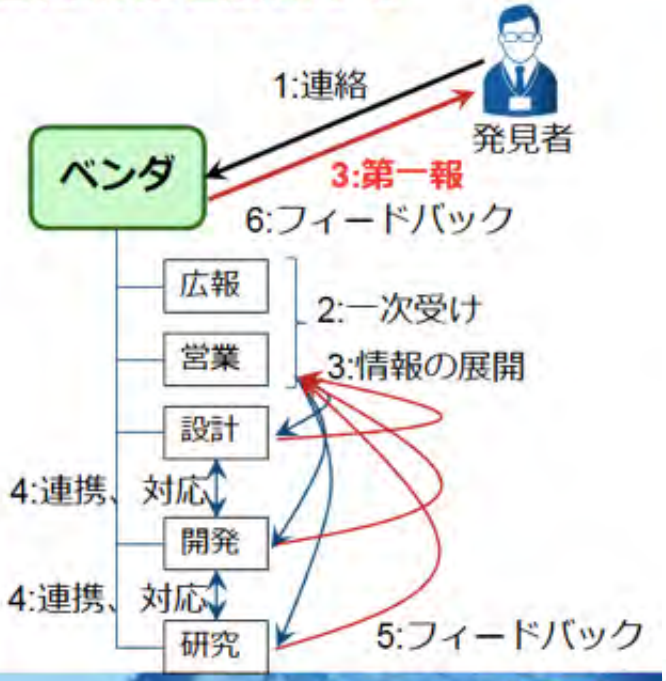
- **IoT では、影響が広い範囲に及ぶケースも考えられる**
  - 製品に脆弱性が発見された場合、ユーザに不安を与えず、冷静に対処してもらうことも重要
  - 業界全体で対応を検討していくことも必要



サイバー攻撃を受けることを前提とした対策の検討が肝要

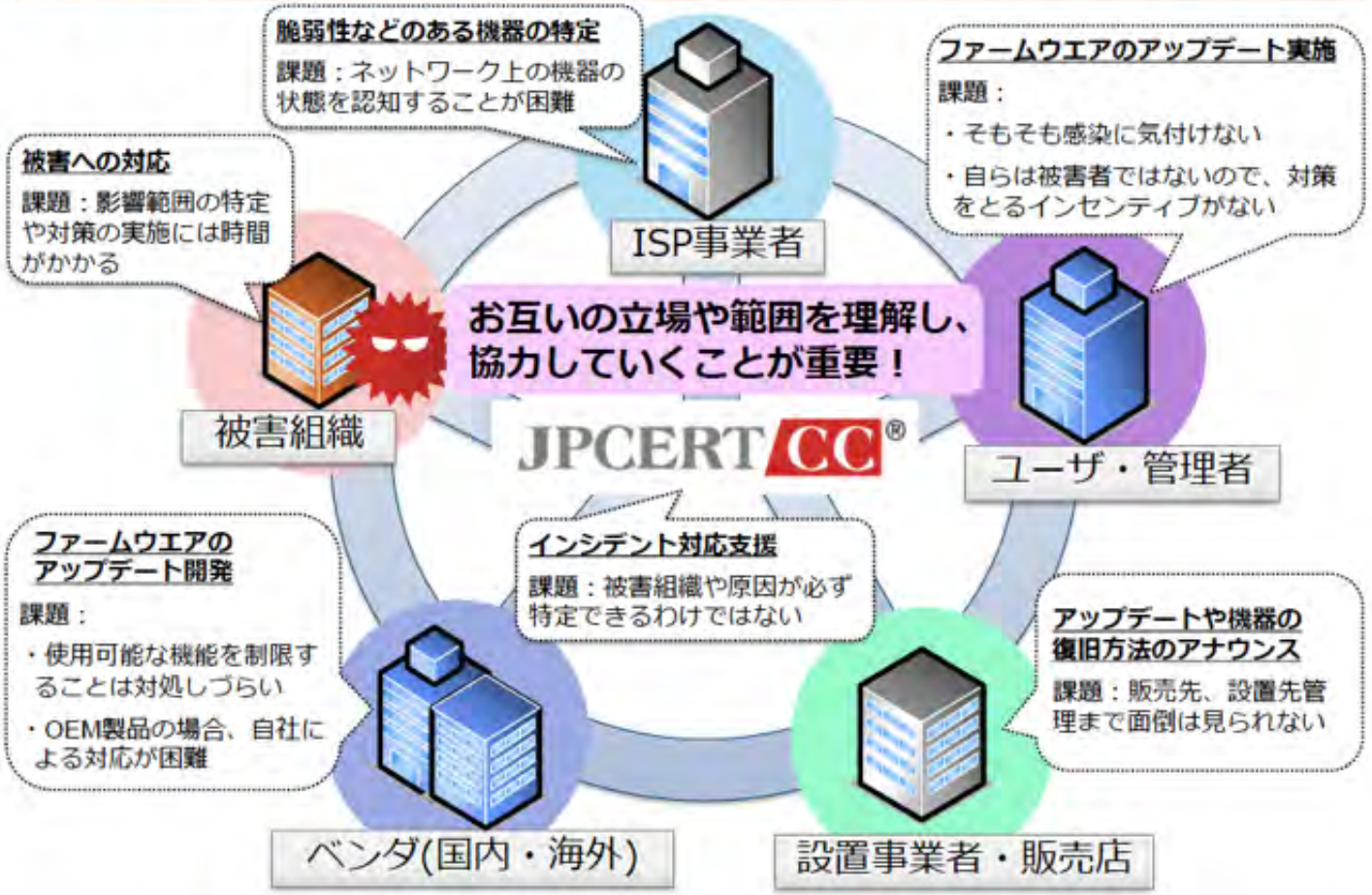
組織内での部門連携の問題

- セキュリティに関する情報が外部から届いたら・・・
  - セキュリティ担当者が直接外部からの情報を受け取るケースは少ない
  - 情報を受け取った人が適切な部署に情報を展開する必要がある
    - 情報のトリアージ
  - さらに内容によって組織内の様々な部門との連携が必要
    - 設計の見直し
    - コード修正、パッチ作成
    - テスト、リリース
    - 発見者への報告



対応完了前に発見者がセキュリティに関する情報(脆弱性の詳細やPoCコードなど)を公開してしまう場合もあるので慎重な対応が求められる

IoT・製品を取り巻くエコシステムにおける課題



IoT全般の課題｜1

IoT機器の課題

- 性能・機能の向上により“スマートな”機器に対する脅威はPCとほぼ変わらない
- 設置された後、適切にメンテナンスされない可能性も考慮する必要がある

Internet of Threatsに関する課題

- IoTには、何かしらの“モノへの制御機能”が備わる
- モノのスケールが大きくなると Cyber-Physical Threatな問題に発展する可能性がある
- インターネットに“モノ”を直接接続することでセーフティに影響が及ばないかを考える必要がある
  - セーフティとセキュリティの両方の観点を考慮する必要がある

業界や関係者で情報共有を行うことの重要性

- **対策を進める上で、PSIRT の構築や、情報共有 (PSIRT間、同業他社、コミュニティ) がカギ**
  - 情報セキュリティの分野では、ISAC (Information Sharing and Analysis Center) による脅威情報の共有が進められている
  - 特に、脅威や影響などに関して共通の話題がある場合には情報共有は進みやすい

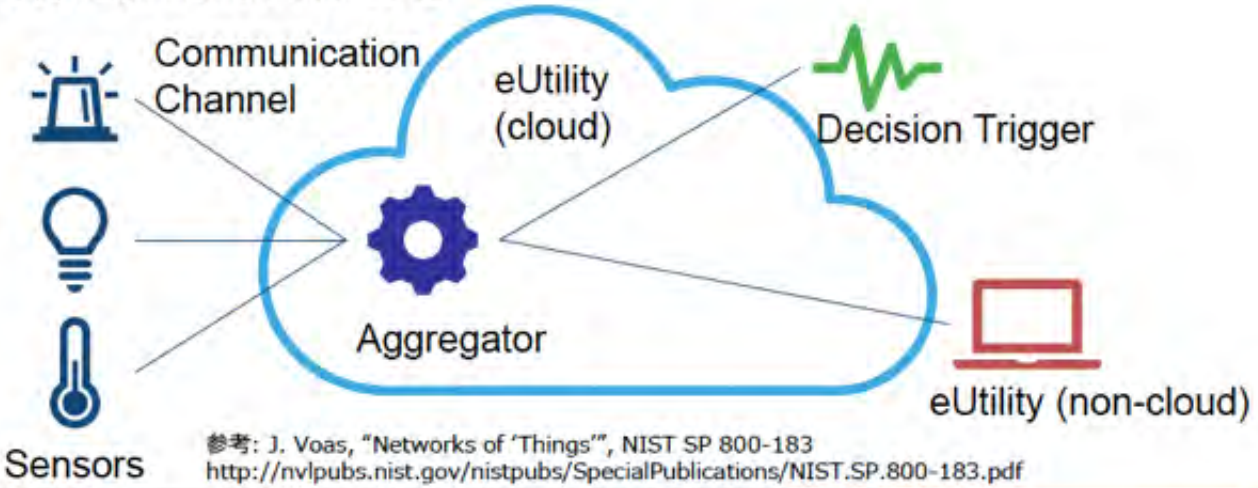
- **コミュニティでの取り組み例**
  - コンシューマ向けIoTセキュリティガイド
    http://www.jnsa.org/result/iot/
    - JNSA IoT セキュリティ WG にてとりまとめ (2016年)
    - 業界を横断して横のつながりで情報を整理
      - セキュリティベンダ、メーカ、その他

コミュニティでの活動がIoTセキュリティをとりまく環境を改善していく上で大きな役割を担うのではないかと考えられる

IoT全般の課題｜2

IoTという言葉で認識する対象範囲の違いによる課題

- IoTの問題は機器だけでなく、クラウド、サーバ、ネットワークなどシステム全体の問題である
- 開発者はそれぞれの立場で自分と繋がる"何か"を意識し、影響を考慮する必要がある
- 開発者 (ベンダ) 、利用者 (ユーザ) 双方がシステム全体の特徴を知る必要がある



参考: J. Voas, "Networks of 'Things'", NIST SP 800-183
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-183.pdf

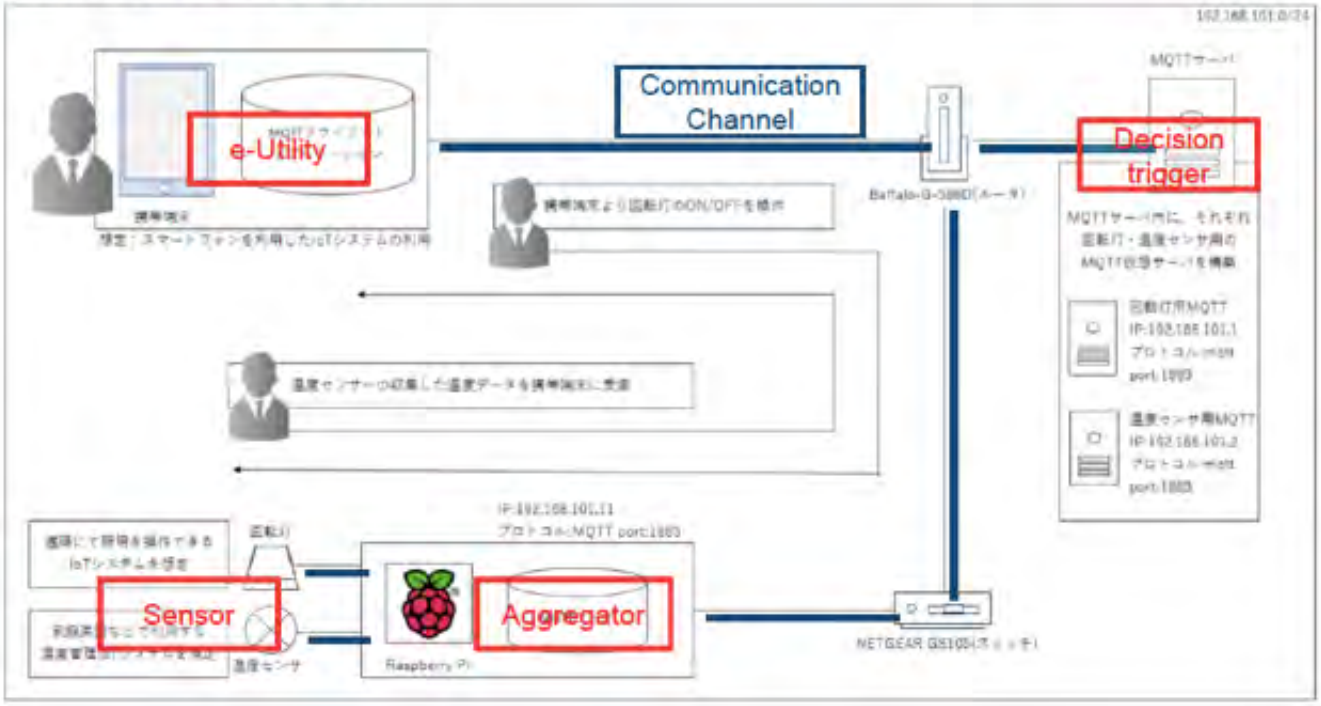
IoT の構成要素

- NIST SP 800-183 によると IoT は以下のように機能ごとに要素を分類できる
  - Sensor：温度、加速度、重量、音、位置などを測定するための機器
  - Aggregator：センサからのデータを集約して処理をする機器
  - Communication channel：データの送受信を行うための通信路
  - eUtility(external utility)：サービスを提供する／受ける機器
  - Decision trigger：データの加工や計算をするための機器

IoTシステムの構成要素ごとの特徴を把握し、それぞれの要素ごとに適切な実装を行っていく必要がある

IoT の構成要素

- 利用している IoT システムのパーツごとの機能を考えて、分類をしてみる



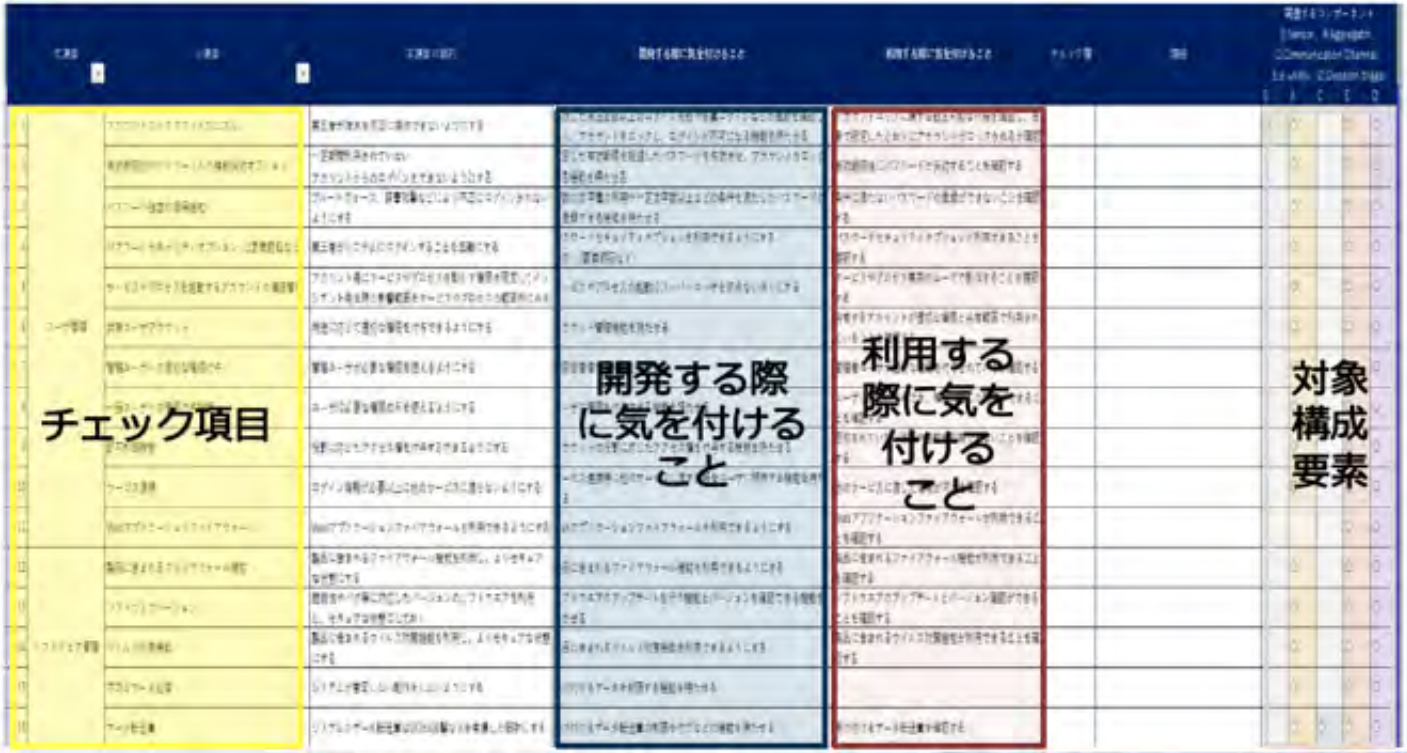
IoT のセキュリティガイドライン

- **IoTに関するセキュリティガイドラインが多く公開されている**
  - IoT にまつわるサイバーでの問題が出始めた 2016 年ごろより国内外の複数の組織より IoT のセキュリティに関するガイドラインが公開されはじめた
  - 公開している組織により対象とする **想定読者**や**レイヤー**に違いがある

ポリシーレベルのガイドラインではなく、運用レベルにフォーカスしたドキュメントの作成を検討した

IoT セキュリティ評価のためのチェックリスト

- 運用レベルでの IoTの脅威と対策を理解するため、
  開発者・利用者双方が確認したい項目をなるべく具体的に
  まとめたチェックリスト を作成中



IoT セキュリティ評価のためのチェック項目

- 複数の IoT、ITのセキュリティのガイドラインを参考に
  確認すべき 7 つの大項目、39 のチェック項目を作成

大項目	チェック項目
ユーザ管理	アカウントロックアウトメカニズム
ソフトウェア管理	有効期限切れパスワードへの強制失効オプション
セキュリティ管理	パスワード強度の担保機能
アクセス制御	パスワードセキュリティオプション（2要素認証など）
不正な接続	サービスやプロセスを起動するアカウントの権限管理
暗号化	共有ユーザアカウント
システム設定	・・・
通知	

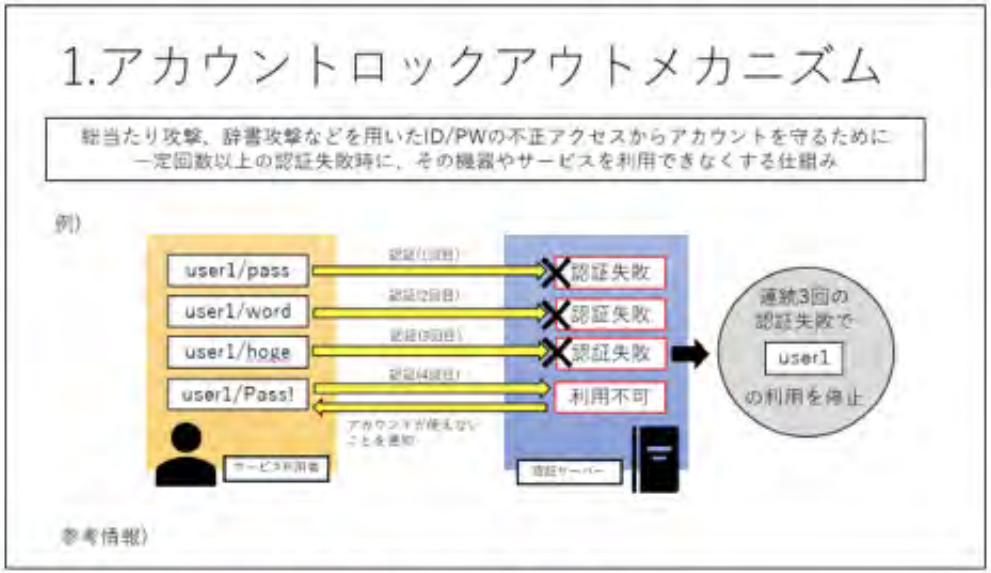
以下のようなガイドラインを参考に要素を抽出

- **IoT Security Guidance**
  - https://www.owasp.org/index.php/IoT_Security_Guidance
- **The Penetration Testing Execution Standard**
  - http://www.pentest-standard.org/index.php/Main_Page
- **The STRIDE Threat Model**
  - https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx

チェック項目のポイント

- **全ての項目を確認する必要はない**
  - — 想定する利用シーンや目的によっては対策を実施しない項目もありうる
  - → 理由を明記し、要件を満たさなくてよい理由を関係者にわかるようにしておく
- **各項目についてイメージしやすいように解説図を添付**
  - — 確認する際にセキュリティに関する言葉がわからない場合がある
  - → 簡単な確認内容とその例を図で説明し、具体的なイメージを持てるようにしている

例：ユーザ管理 / アカウントロックメカニズム



第三者が端末を不正に操作できないようにする

- **【開発の際に気を付けること】**
  連続した規定回数以上のログイン失敗や多重ログインなどの痕跡を確認したら、アカウントをロックし、ログインが不可になる**機能を持たせる**
- **【利用する際に気を付けること】**
  アカウントロックに関する**設定可能な内容を確認**し、自身で設定したとおりにアカウントがロックされるか確認する

IoTを構成する要素ごとの評価

- デバイスだけを評価すればいいわけではない
  - — NIST SP 800-183 に定義されている IoT の構成要素
    (Sensor, Aggregator, Communication Channel, e-utility, Decision trigger)
  - — IoT の構成要素ごとに確認すべき項目を抽出

チェック項目
アカウントロックアウトメカニズム
有効期限切れパスワードへの強制失効オプション
パスワード強度の担保機能
パスワードセキュリティオプション（2要素認証など）
サービスやプロセスを起動するアカウントの権限管理
共有ユーザアカウント
・・・

本項目は次の構成要素となる製品が確認
- Sensor
- Aggregator
- e-utility
- Decision trigger

本項目は次の構成要素となる製品が確認
- Aggregator
- e-utility
- Decision trigger

活用

本チェックリストの対象者は

- **IoT の製品開発者**
- **ビジネスレベルの IoT の製品利用者**
  - **ある程度の IT などの知識が必要**

どんな場面で本チェックリストを使うのか

- **例：製品開発時の要件のチェック**

  開発工程の各段階の仕様確認の際に確認
  - **設計段階で特に確認したい項目を選んでおく**

    確認したい項目を満たしているか各工程の確認者が改めて確認をする

課題

- **公開に向けて作成したチェックリストについて意見を募集しています**
  - — 現在の項目数に抜け漏れがないか確認をしたい
    - 今回作成した基本的な項目の他に足りないものがあるかもしれない
  - — セキュリティの観点からリストを作成している
    - ITのセキュリティに関する知識と製品側のセキュリティ(セーフティ)に関する知識は大きく違うのかもしれない

まだまだ、多くの方に意見を頂いていく必要がございます。
チェックリストの評価など興味を持たれた方は、
ぜひ会話させてください

http://www.jnsa.org/seminar/2018/0226/index.html

KASPERSKY lab

まとめ

IT、OT、ICS、Embedded systemなどの言葉に惑わされないこと

まとめ

- IISFにも記述があるが、セキュリティの要件は例外が多すぎる上に増え続けることが課題
- インクリメンタルに、出荷後にも追加のテストとシステムの更新が可能でなければならない
- ホワイトボックステストで既知の脆弱性を排除、これはツールも出始めている
- システムテスト（ペンテスト）でシステムレベルの脆弱性を排除できるとうれしい
- セキュリティ専業ベンダーのアセスメントを受けるのも一つの解決策

KASPERSKY

ご静聴ありがとうございました

masato.matsuoka@kaspersky.com

KASPERSKY lab